WatchDOG® Elite

Quick Start Guide

Watch List Screening

Policies and Procedures

SmartRisk IQ

Vendor Management

Controls and Response

CONFIDENTIAL

CSI Regulatory Compliance
13860 Ballantyne Corporate Place
Suite 200
Charlotte, NC 28277
Telephone 888-494-8449

Copyright © 2015 CSI

WatchDOG® Elite

Quick Start Guide

CONFIDENTIAL

The information in this document is confidential and is proprietary to CSI. It is intended solely for the addressee. Access to this document by anyone else is unauthorized. If you are not the intended recipient, any disclosure, copying, or distribution or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful. If this document is received by anyone other than the addressee, please contact CSI Regulatory Compliance at 888-494-8449. Thank you.

Table of Contents

INTRODUCTION 1

About This User Guide 1
Watch List Screening *1*
Policies and Procedures (P&P) *1*
SmartRisk IQ *2*
Vendor Management *2*
User Guide Conventions *2*
Additional Documentation *3*
System Requirements 4
Supported Browsers *4*
Browser Settings *4*
Monitor Resolution Settings *4*
Third Party Applications *4*
Logon 5
Session Timeout 6
Introduction to the Home Page 6
Defining User Preferences 7
Steps to modify the User Preferences *8*
Introduction to the Navigation Toolbar 9
Self-service Reset Passwords *10*

WATCH LIST SCREENING OVERVIEW 12

Transaction Details Overview 12
Options to navigate through the transaction list *13*
Up/Down Arrows 13
Transaction List Navigation 14
Reviewing the Watch List Transaction Details *14*
Transaction Details for Non-Exact ID Match Screening 14
Transaction Details for DMF Screening 15
Transaction Details for NPI Screening 16
Transaction Details Options menu *17*
Print the Transaction Detail Report 17
Add the matched item as a Workflow Item 18
Upload an attachment 20
View an attachment 21
Delete an attachment 21
Reviewing the Transaction Filter Status and Source Data *22*
Steps to assign a matched item to the GCL, BCL or Reviewed Status 23
Screen a Single Item Overview 25
How to screen a single item *25*
Screening a Sanctioned Country 26
Screening on Exact ID Match 27
Reviewing the results of the single item screening *27*
Screen a Batch File Overview 28
Steps to submit a batch file for screening *28*

CONFIDENTIAL

REVIEW BATCH FILE RESULTS 30
Steps to search and retrieve completed batch results *30*
Reviewing the results of the single a single item screening 31
Batch Options *31*
Steps to add Batch Comments 32
Steps to Close a Batch 33
Steps to Lock a Batch 34
Steps to Unlock a Batch 35
Batch Reports *35*
Steps to run the Batch Run Report 35
Steps to run the Detailed (Batch) Report 36
Steps to run the Statistics Report 38
Steps to run the Audit Report 38
REVIEW TRANSACTIONS OVERVIEW 39
Steps to search for a previously screened item *39*

POLICIES AND PROCEDURES OVERVIEW 42

CREATING A P&P DOCUMENT CATEGORY 42
Editing a P&P Document Category *44*
MANAGING A P&P DOCUMENT 44
Creating a Document *44*
Viewing the Manage P&P Documents Grid *48*
Viewing Document Details and Editing a Document *48*
Publishing a Document that does not Require Approval *50*
Publishing a Document that Requires Approval *50*
Creating a New Version of a Document *50*
Archiving a Document *53*
Viewing a Document's Version History *53*
P&P DOCUMENT REVIEW FOR USERS 54
Viewing Documents for Acceptance *54*
P&P REPORTING 56
Document Summary Report *56*
User Document Action Report *56*
Document Audit Report *56*
Document Detail Report *56*
DOCUMENT LIBRARY 56
Document Library Search *57*

SMARTRISK IQ OVERVIEW 58

RISK MANAGEMENT SETTINGS 58
Category Risk Appetite *59*
Risk Appetite Audit Report *60*
RISK CATEGORIES 61
KEY RISK INDICATORS 62
Manage Key Risk Indicators *62*
Key Risk Indicator Details *64*
Key Risk Indicators on Assessments *66*
Key Risk Indicator Reports *67*

CONFIDENTIAL

Key Risk Indicator Audit Report (Export) 67
Key Risk Indicator Summary Report 68
RISK ASSESSMENTS 69
Create a New Risk Assessment *69*
Risk Assessment Details *71*
Risk Assessment Category Questions *73*
Opting Out of Questions *74*
Edit Assessment Details *75*
Finalize Assessment *76*
Risk Calculations *77*
Assessment Question Risk Levels 77
Category Risk Levels 78
Assessment Risk Levels 78
SMARTRISK IQ REPORTING 78
Risk Assessment Detail Report *78*
Assessment Audit Report *79*
Assessment Executive Report *79*
Assessment Question Detail Report *79*
Assessment Summary Report *79*
Risk Appetite Trend Report *79*
VENDOR MANAGEMENT OVERVIEW 81
VENDOR CATEGORIES – CREATE AND MANAGE 82
Editing a Vendor Category *83*
VENDOR OPERATIONAL AREAS – CREATE AND MANAGE 84
Creating an Operational Area *84*
VENDORS – CREATE AND MANAGE 85
Create and manage the Vendor Demographics *85*
Add Vendor Contacts 88
Edit Contact Information 89
Delete a Contact 90
Assign Dependencies 91
VENDOR ASSESSMENTS – CREATE AND MANAGE 92
Introduction to the Assessment Details page *94*
Questions/Answers 94
Intelligent Content 95
Uploading Attachments to questions 96
Steps to upload an Attachment 96
Review the Attachment 97
Assessment Question Comments 99
Assessment Options Menu 100
Vendor Assessment Detail Report 100
Edit Assessment Details 101
Finalize Assessment 102
VENDOR CONTRACTS 103
Steps to create a contract entry 103
Steps to upload an Attachment 104
Review the Contract Attachment 106
View all Vendor related Attachments *107*

CONFIDENTIAL

Vendor Notes *107*
VENDOR REPORTS 108
Assessment Audit Report *108*
Assessment Question Detail Report *108*
Assessment Summary Report *108*
Contract Audit Report *108*
Contract Summary Report *108*
Demographic Audit Report *108*
Demographic Summary Report *108*
Vendor Summary Report *109*
Vendor Batch Screening Report (Export) *109*
Vendor Batch Screening Contacts Report (Export) *109*
TECHNICAL SUPPORT AND CONTACT INFORMATION 121

CONFIDENTIAL

Introduction

Welcome to WatchDOG® Elite. This application allows users to perform the essential functions of an effective regulatory compliance program, including conducting restricted party watch list screening, creating and managing policy and procedure review and acceptance, completing risk assessment activities across the enterprise, and managing third-party vendor relationships.

- Watch List Screening facilitates restricted party screening process using data entered via a web browser or by automated integration to meet your compliance needs.
- Policies and Procedures enable you to comply with creating and tracking policy acceptance practices.
- SmartRisk IQ facilitates baseline and ongoing risk assessment activities across the enterprise.
- Vendor Management helps automate and streamline the oversight of vendor relationships.
- Controls and Response enable users to log and track findings, matters, issues, and tasks related to Regulatory Compliance activities as part of the control, remediation and response process.

About This User Guide

This *Quick Start Guide* describes a subset of the full feature functionality of the application, from the end user's perspective; however, only the service(s) and features to which your institution subscribes are available to you in the application. In this document, the following functionality will be reviewed:

Watch List Screening

- Password Resets
- Defining User Preferences
- Screening a Single Name
- Screening a Batch File
- Retrieving the Batch Results
- Managing the Screened Transactions

The Product Documentation contains a full set of features and functionality, including the Administrative setup, can be accessed via the Product Documentation link (in the Navigation toolbar).

Important Note: For institutions who subscribes to web services or FTP integration, a separate document will be provided to outline the instructions for screening single names and batch files.

The manual is written with the assumption that the user has full access to all features and functionality. Depending on your access, certain features and functionality may not be available to you.

Policies and Procedures (P&P)

- Creating and editing Categories associated to the policies and procedures documents
- Creating P&P Documents
- Approving Documents
- Publishing P&P Documents
- Archiving Documents

CONFIDENTIAL

- End User review of the document(s)
- Reporting

SmartRisk IQ

- Reviewing Categories associated with Risk Assessments
- Setting risk tolerance levels by Risk Category
- Managing Key Risk Indicators
- Creating and managing Risk Assessments
- Uploading attachments and making notes for Risk Assessments
- Accessing Risk Management Reports

Vendor Management

- Creating and editing Categories associated with Vendors
- Creating and editing Operational Areas associated with Vendors
- Creating and managing Vendors
- Creating and managing Vendor Assessments
- Creating entries for Vendor Contracts
- Uploading attachments and notes to Vendors
- Accessing Vendor Reports

Controls and Response

- Creating and editing Categories within Issue Center
- Creating and managing Issues
- Adding and editing comments as issues are in progress
- Uploading and managing attachments
- Accessing Issue Reports

User Guide Conventions

The user guide uses the following conventions to relate information.

Buttons, Links, Fields, Pages, Windows

- Buttons/Links: Where mentioned, the buttons and links are in a bold font.
- Fields: Field names are capitalized; i.e. – Individual Name field.
- Pages and Windows: Referenced as capitalized, such as Batch Results page.

CONFIDENTIAL

Additional Documentation

A full user reference manual is available via the Product Documentation link in Navigation toolbar.

CONFIDENTIAL

System Requirements

WatchDOG Elite requires the following:

Supported Browsers

- Internet Explorer version 9, 10 and 11 (all in native mode), Chrome and Firefox

Browser Settings

Browser configured to support:

- Cookies. Allow cookies; verify that "Always allow session cookies" is checked.
- Pop-ups. Allow pop-ups; verify that "Block pop-ups" is unchecked.

  Note: Browser configuration settings for IE are located in Tools>Internet Options. Follow the menu options for your version.

Monitor Resolution Settings

- Optimized screen resolution for WatchDOG Elite is 1152 x 864 and higher. The lowest resolution supposed is 1024x768; however, this could require additional scrolling within the application to view all data and fields.

Third Party Applications

- Adobe Reader version 9 or higher (to reports and other documents as PDF)

CONFIDENTIAL

Logon

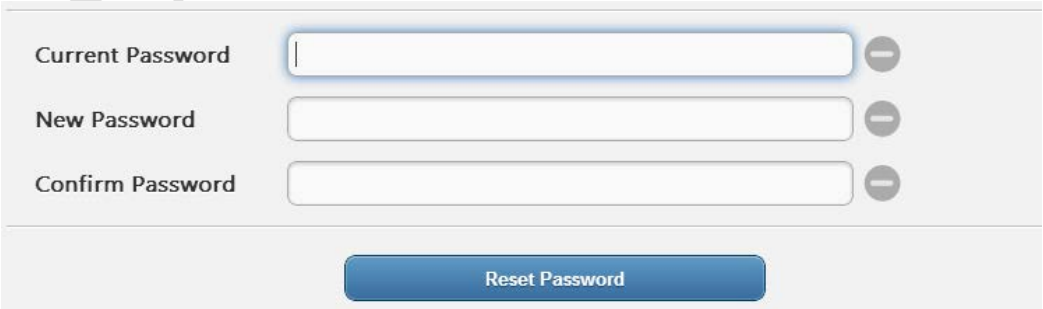
The login page consists of three login fields, an option to have the system remember the Company and User ID for subsequent logins as well as an option to reset the password, if forgotten.

1. At the logon window, enter your Company, User ID, and Password.

   Company and User IDs are not case sensitive; however, the password is case-sensitive.

   Remember Me: Uncheck this box to not have your logon credentials retained for subsequent visits to this website.

2. Click **Logon** to launch the WatchDOG Elite Home page.
3. Upon initial login, the default password expires and you must create a new password.



CONFIDENTIAL

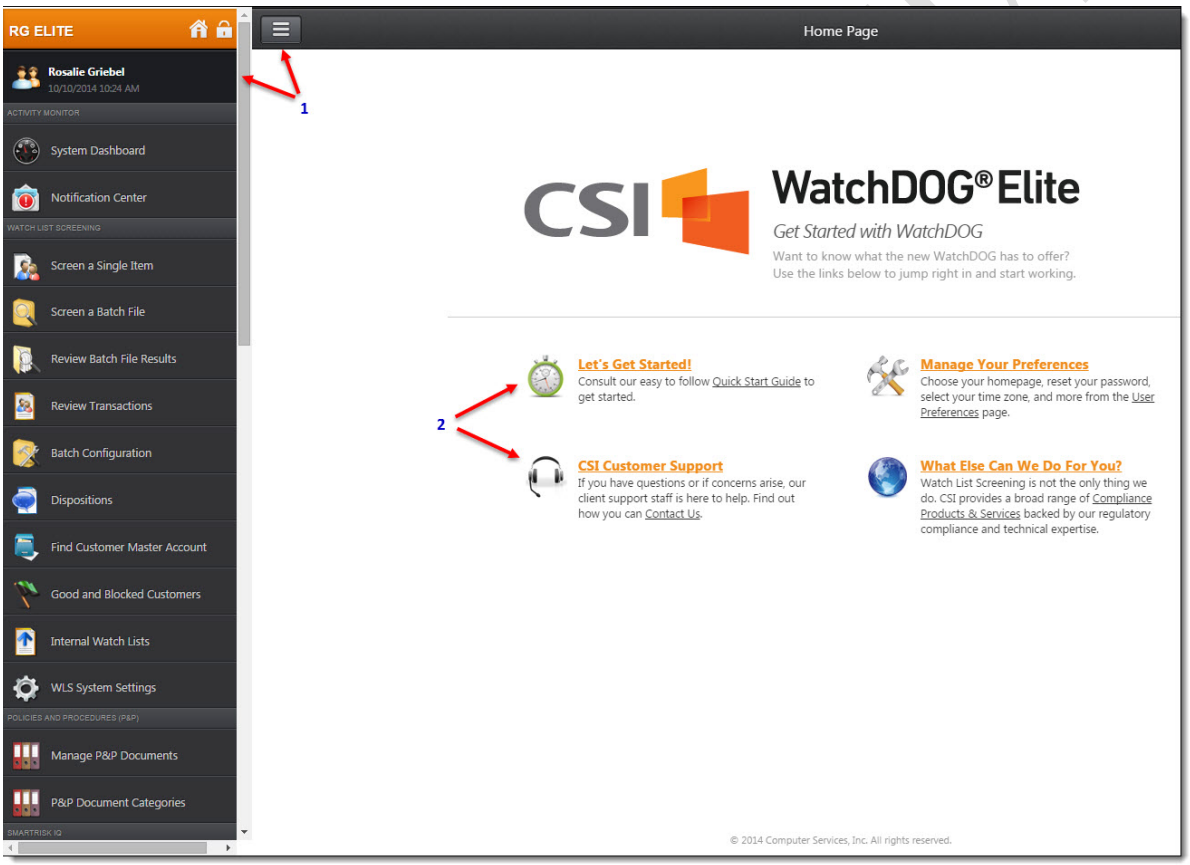
4. Enter the current password, and then enter the new password in the New Password and Confirm Password fields, making sure to follow the requirements that display to the right of the password entry field.
5. Click **Reset Password**. You will then be directed to the default Home Page.

Session Timeout

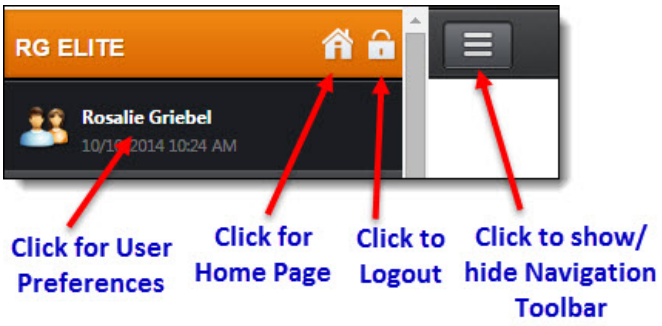
After 20 minutes of idle time, the application session will timeout. When you attempt to resume work, you will be directed back to the login page. Upon successfully logging in, you will be directed to the page where you timed out.

Introduction to the Home Page

By default, the Getting Started page serves as the user's Home Page. Later, you will learn how a user can define their Home Page.


RG ELITE
Rosalie Griebel
10/10/2014 10:24 AM
ACTIVITY MONITOR
System Dashboard
Notification Center
WATCH LIST SCREENING
Screen a Single Item
Screen a Batch File
Review Batch File Results
Review Transactions
Batch Configuration
Dispositions
Find Customer Master Account
Good and Blocked Customers
Internal Watch Lists
WLS System Settings
POLICIES AND PROCEDURES (P&P)
Manage P&P Documents
P&P Document Categories
SMARTRISK IQ
Home Page
1
2
CSI
WatchDOG® Elite
Get Started with WatchDOG
Want to know what the new WatchDOG has to offer?
Use the links below to jump right in and start working.
Let's Get Started!
Consult our easy to follow Quick Start Guide to get started.
Manage Your Preferences
Choose your homepage, reset your password, select your time zone, and more from the User Preferences page.
CSI Customer Support
If you have questions or if concerns arise, our client support staff is here to help. Find out how you can Contact Us.
What Else Can We Do For You?
Watch List Screening is not the only thing we do. CSI provides a broad range of Compliance Products & Services backed by our regulatory compliance and technical expertise.
© 2014 Computer Services, Inc. All rights reserved.

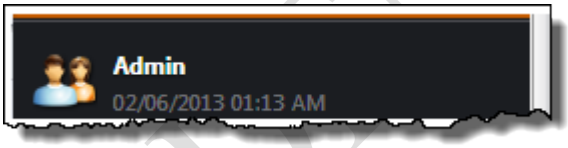
1. This top section contains the options to do the following:
   - Access to User Preferences
   - Home Page
   - Logout
   - Show/Hide Navigation toolbar



2. Use the links on the Home Page to access the following:
    - Quick Start Guide
    - User Preferences
    - Customer Support
    - Review our product offerings

Defining User Preferences

This link identifies the current user and the last time they logged into the application.



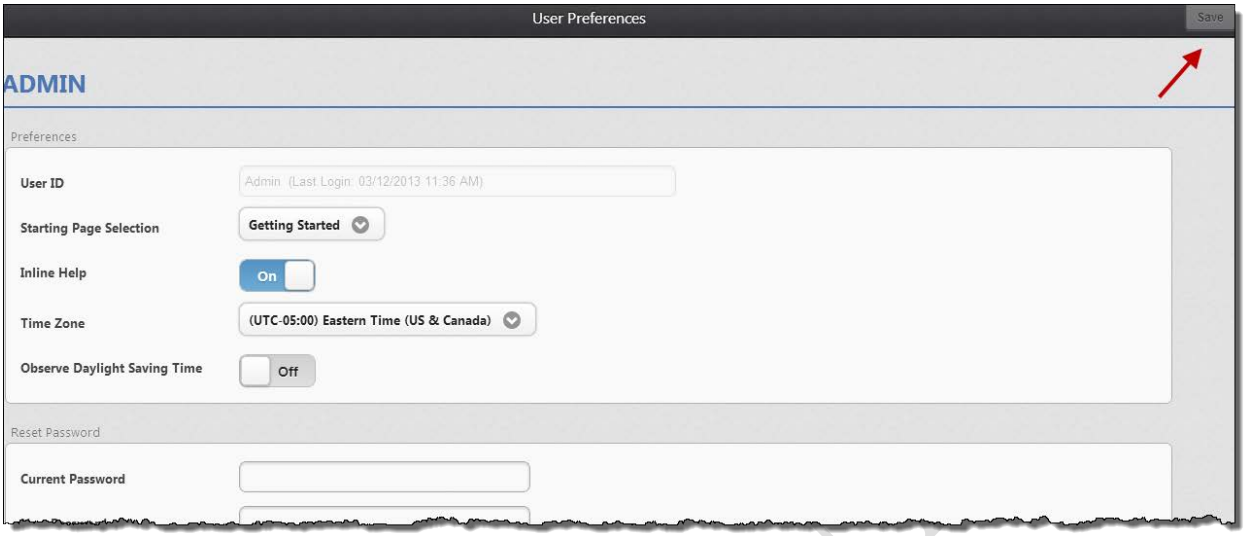
When this link is selected, the User Preferences page is presented where the user can make applicable changes such as:

- The ability to select the user's default Home Page. The Getting Started page is the default Home Page. If a new default is not set, upon subsequent login, the user will be taken to the last page used prior to logoff;
- Elect to turn Inline Help on or off. If set to On, help and error messages will display to the right of fields, when/where applicable;
- Select the user's Time Zone. The user's time zone will be reflected in most of the grids and reports. The exception is in all comments fields and the user login and audit pages;
- Indicate if Daylight Saving Time is observed

CONFIDENTIAL

Steps to modify the User Preferences

1. Select the **User Preferences** link.
2. Modify the settings such as the Starting Page and Time Zone.



3. After making the application changes, select the **Save** button.

CONFIDENTIAL

Introduction to the Navigation toolbar

The Navigation pane on the left side of the page contains links to the various application functions, based on the security roles assigned to the currently logged in user.

The company and user id of the currently logged in user is displayed at the top of the pane; via this link, the user can reset the password.

The toolbar is separated into the following sections:

- Activity Monitor
- Watch List Screening
- Policies and Procedures
- SmartRisk IQ
- Vendor Management
- Controls and Response
- Workflow
- System Reports
- System Administration
- Documentation

CONFIDENTIAL

Self-service Reset Passwords

Via the Challenge/Response feature, end users have the ability to reset forgotten passwords.

To take advantage of the self-service reset password feature, first supply your Company and User ID, and then click on the Forgot Password link via the Logon page.

Upon selecting the link, a challenge question will be displayed.

CONFIDENTIAL

If the user answers this correctly, then the Reset Password page will be displayed where the user can enter a new password.

Once the user successfully creates a new password, they will be automatically logged in to the application.

If the user does not answer the first challenge question correctly, then a second question will be provided. The user has a total of three chances to answer a single randomly selected question in order to advance to the Reset Password page.

If the user fails all questions, then the user needs to contact their system administrator.

If the user selects the Back button, the focus will return to the login page.

CONFIDENTIAL

Watch List Screening Overview

In this chapter, the Watch List Screening section of the Navigation toolbar will be reviewed. The Watch List Screening features contains tools necessary to screen single items, screen batches of items, and review/report on any matches via the user interface. If your institution submits single lookups via web services or batches via FTP, you will be provided a separate document of instructions.

Following is a list of Watch List Screening topics and functionality addressed in this section:

- Explanation of a Transaction
- Steps to screen a single item
- Steps to upload a batch file containing data for your customers, vendors, etc.
- How to access and manage the results of a batch screening
- How to search and retrieve a previously searched item
- Add names to the Good and Blocked Customer Lists
- Managing the Internal Watch Lists

Transaction Details Overview

A transaction is a unit of work where the name, address, country, or identifier is screened against one or more watch lists. Each transaction has a system assigned unique id (referred to as the Transaction ID).

The screening results for the transaction are viewed via the Transaction Details page where the possible match is used to compare the input data to the possible entity match to determine a true or false possible match. Once a determination has been made, the input name can be added to the Good Customer List, the Blocked Customer List or flagged as a Reviewed status. In addition, a disposition can be assigned to the item to indicate the reason as to why it is or is not a true match.

Regardless of the screening method, the actions to resolve the possible match are available on the Transaction Details page, if a unique id is supplied.

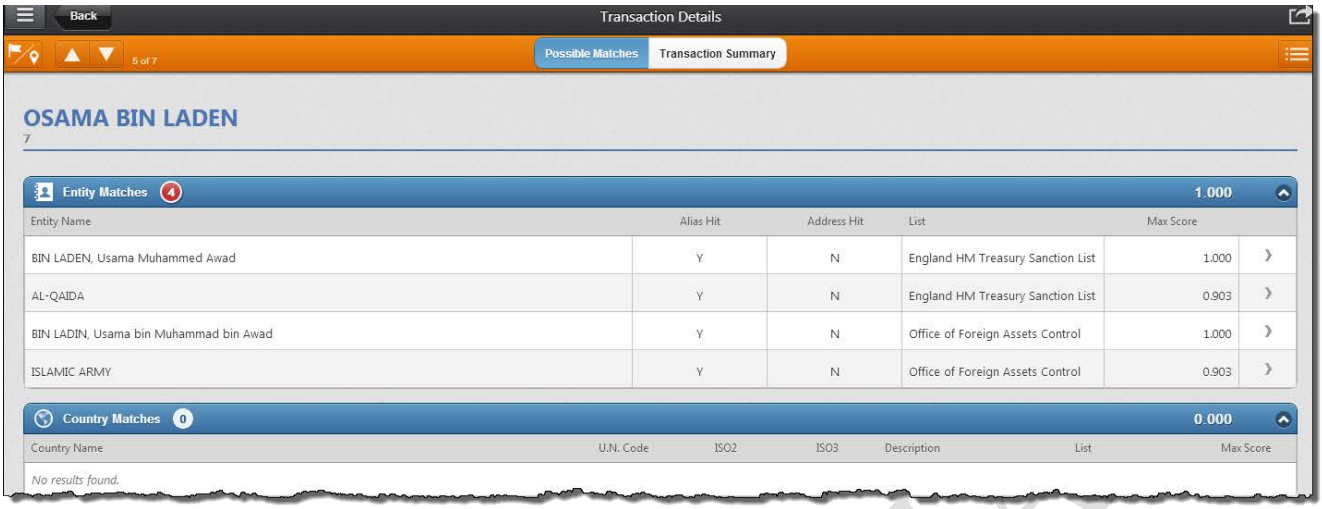
> **Important Note:** names screened via the Screen a Single Item page cannot be added to the GCL or BCL.

The Transaction Details page is accessible via the following pages:

- The results of screening a single item
- Batch Results page
- Review Transactions

The following example illustrates a search on a Full/Partial Name of “Osama bin Laden” against the OFAC and the HM Treasury watch lists. The Entity Matches section shows the name matches where there are four (4) matches highlighted in the red circle.

CONFIDENTIAL



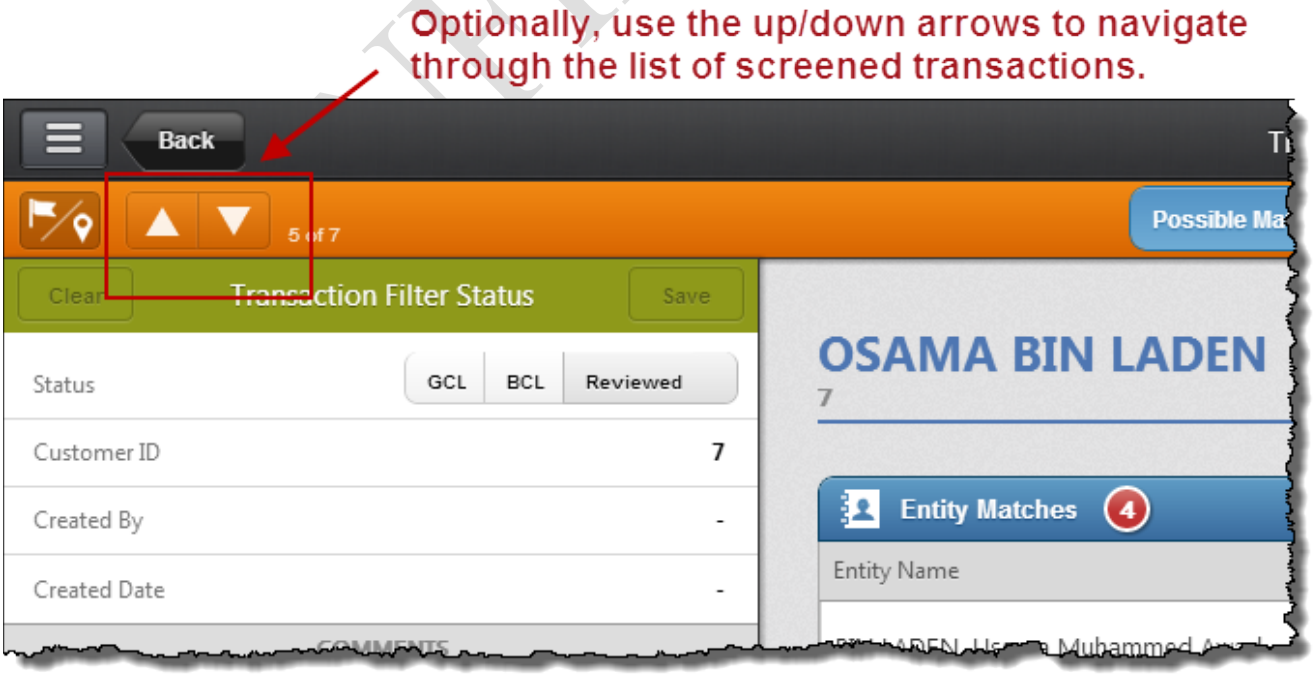
Options to navigate through the transaction list

From the Transaction Details page, there are two methods in which to optionally navigate through the list of transactions.

- Up/Down Arrows
- Transaction List icon

Up/Down Arrows

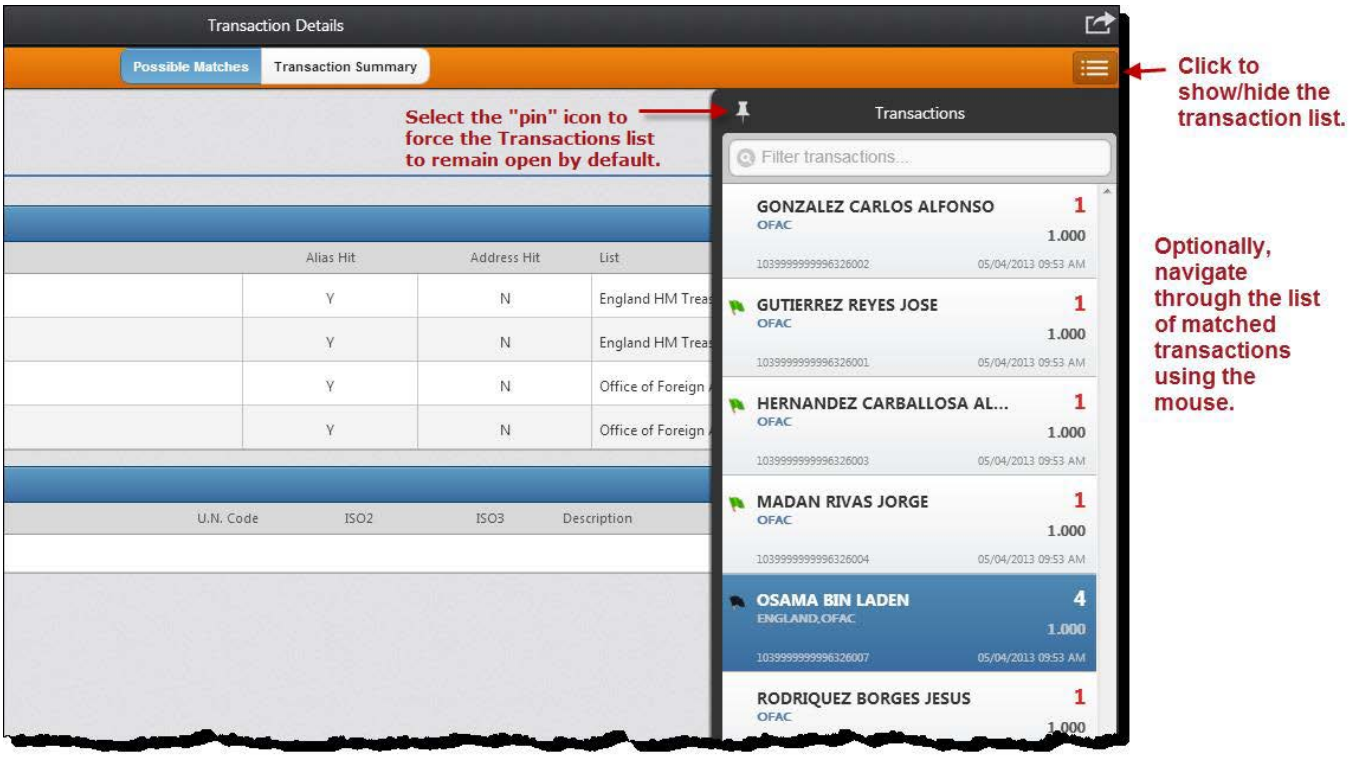
For batch results only, the arrows on this page are visible to the user. Simply click the applicable arrow icon to navigate through the list of matched transactions.



CONFIDENTIAL

Transaction List Navigation

Use this icon to show/hide the list of transactions. The list of transactions is based on the search criteria from the Batch Results or Review Transactions grid.



Reviewing the Watch List Transaction Details

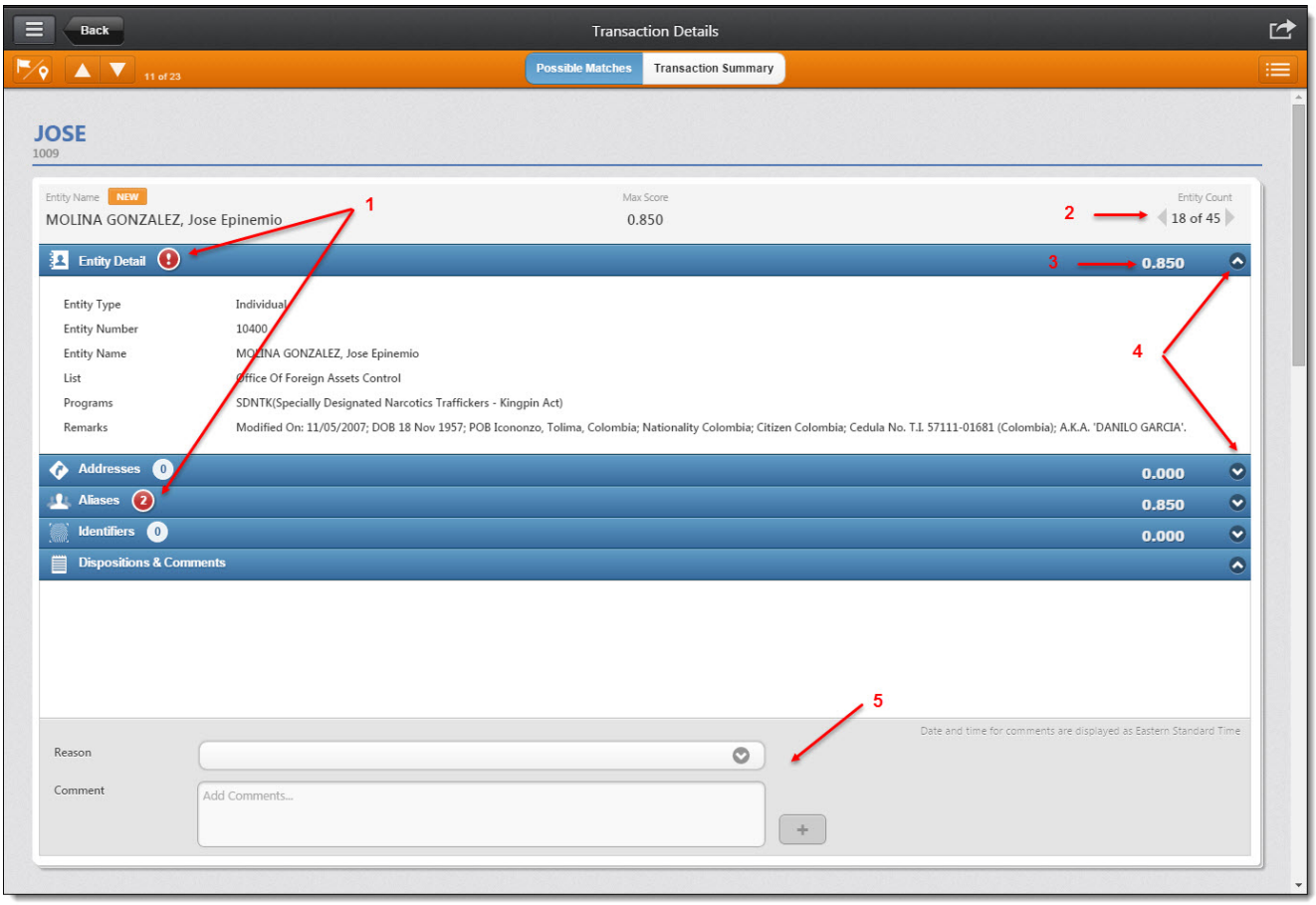
As part of the review and resolve process, you may drill into the details of the watch list transaction by clicking on the row of the matched item. From this level, the watch list transaction, any related alias and address information is available to be used as part of the review process.

The actual review process and the entity details for the transaction varies based on the type of item screened.

Transaction Details for Non-Exact ID Match Screening

Referencing the numbers in the following image, let's learn about the composition of the Transaction Details page for Individuals, Non-Individuals, Sanctioned Countries, and Type Unknown screened items.

CONFIDENTIAL

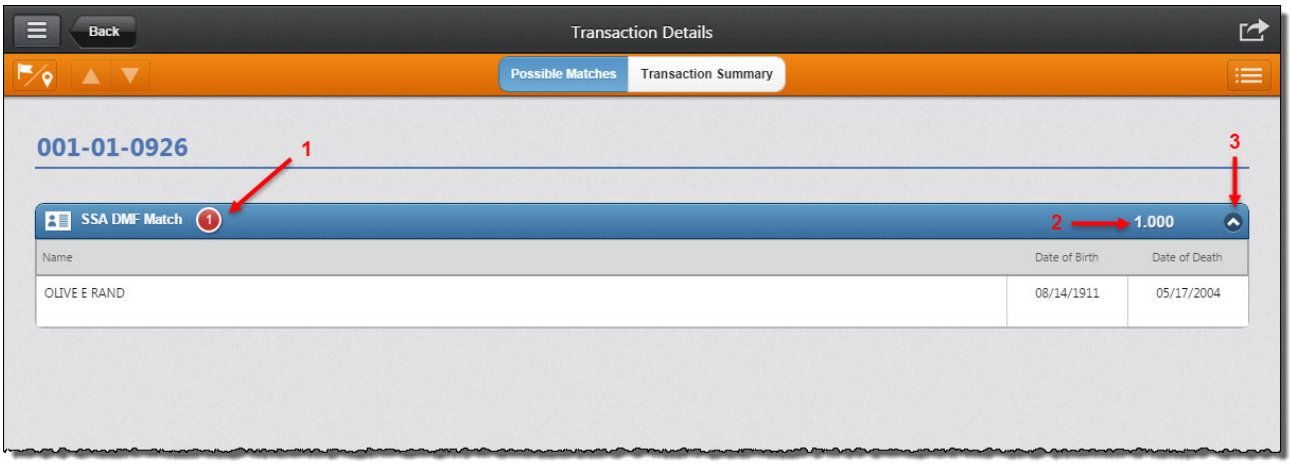


1. The red circles indicate that these sections contain entity information that matched at or above the screened threshold.
2. Identifies the number of entity matches for the selected matched item. Each entity should be reviewed.
3. Indicates the threshold (or score) in which the input item matched against the watch list data.
4. Use the icon to expand/collapse the section.
5. A disposition reason and comments may be assigned. A reason is assigned to identify why the matched item was or was not a true match.

Transaction Details for DMF Screening

Referencing the numbers in the following image, let's learn about the composition of the Transaction Details page for Exact ID Match screening against the SSA DMF (Death Master File) list.

CONFI

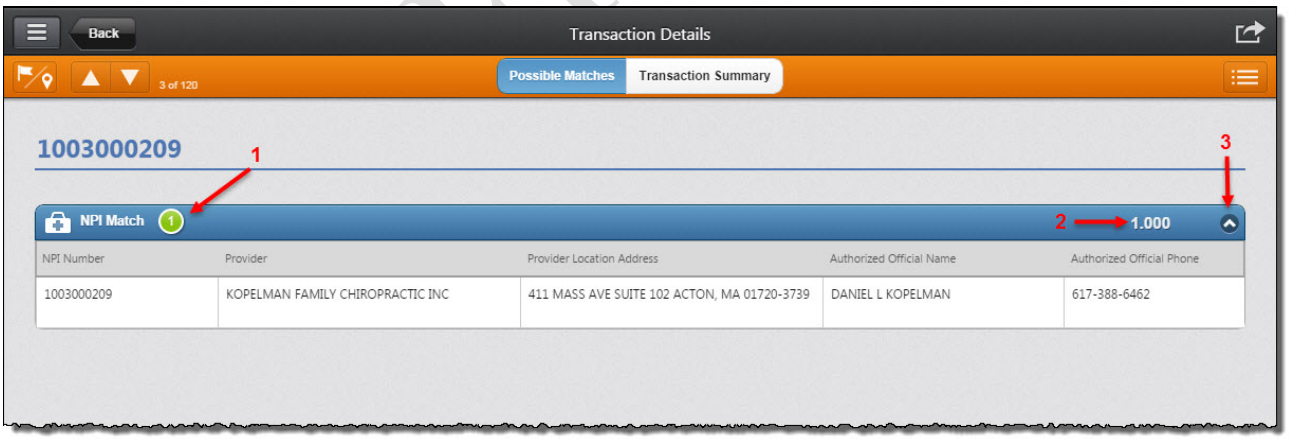


1. The red circle indicates that there was a match for the SSN entered in the search to the SSA DMF list. If there is not a match, a gray circle with a zero (0) will appear. The number of matches will always be either 1 (match) or 0 (no match).
2. Indicates the score for which the input item matched against the watch list data. This will always either be 1.000 for a match or 0.000 for no match. There are no thresholds since these are all an exact match in the ID entered.
3. Use the icon to expand/collapse the section.

   Important Note: There are no individual entity details for SSA DMF Match, so there is no disposition or comments section for these transactions.

Transaction Details for NPI Screening

Referencing the numbers in the following image, let's learn about the composition of the Transaction Details page for Exact ID Match screening against the NPI (National Provider Identifier - number) registry.



1. The green circle indicates that there was a match for the NPI entered in the search to the NPPES (National Plan & Provider Enumeration System) NPI registry. If there is not a match, a gray circle with a zero (0) will appear. The number of matches will always be either 1 (match) or 0 (no match).
2. Indicates the score for which the input item matched against the watch list data. This will always either be 1.000 for a match or 0.000 for no match. There are no thresholds since these are all an exact match in the ID entered.

CONFIDENTIAL

3. Use the icon to expand/collapse the section.

   Important Note: There are no individual entity details for NPI Match, so there is no disposition or comments section for these transactions.

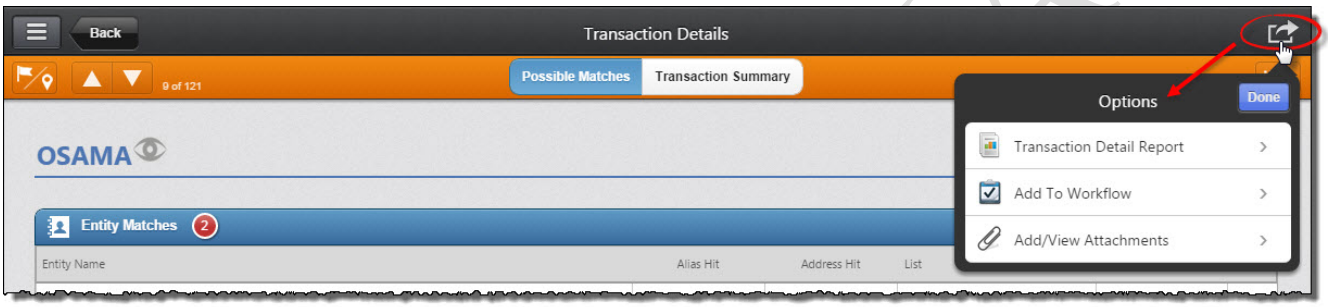
Transaction Details Options menu

Within the Options menu, there are options to print the Transaction Detail Report, add the transaction to as a workflow item, and Add/View Attachments.

The Detail Report presents a printable version of the screened data and the match information as well as all the criteria used to screen the item.

The Add To Workflow option allows the assignment of the transaction to another user of the system for review. An email notification will be sent to the assigned person making them aware of the task.

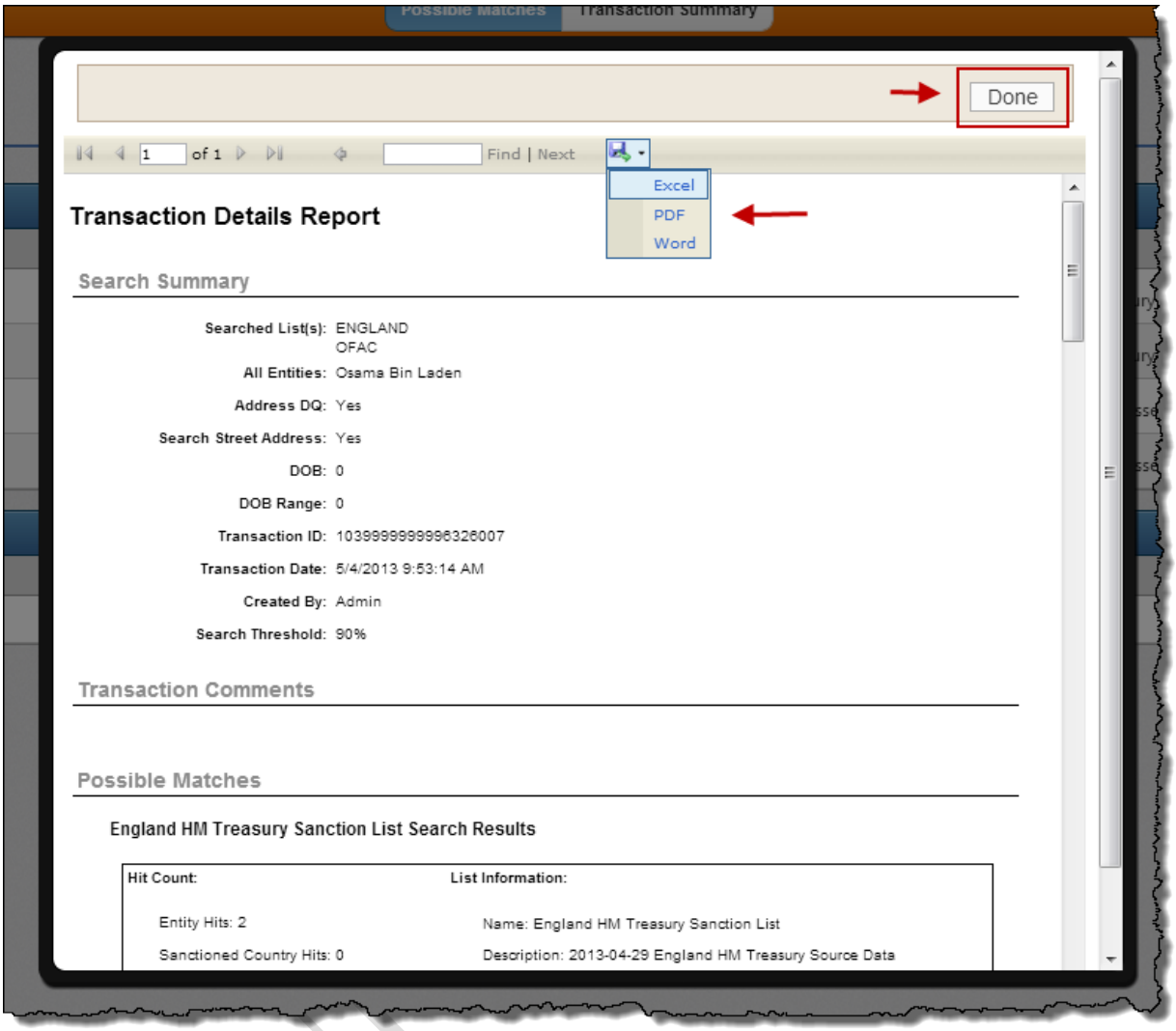
Add/View Attachments enables users to upload and then view supporting documents for the transaction.



Print the Transaction Detail Report

1. From the Options menu, select **Transaction Details Report.** The report will load in a separate window.

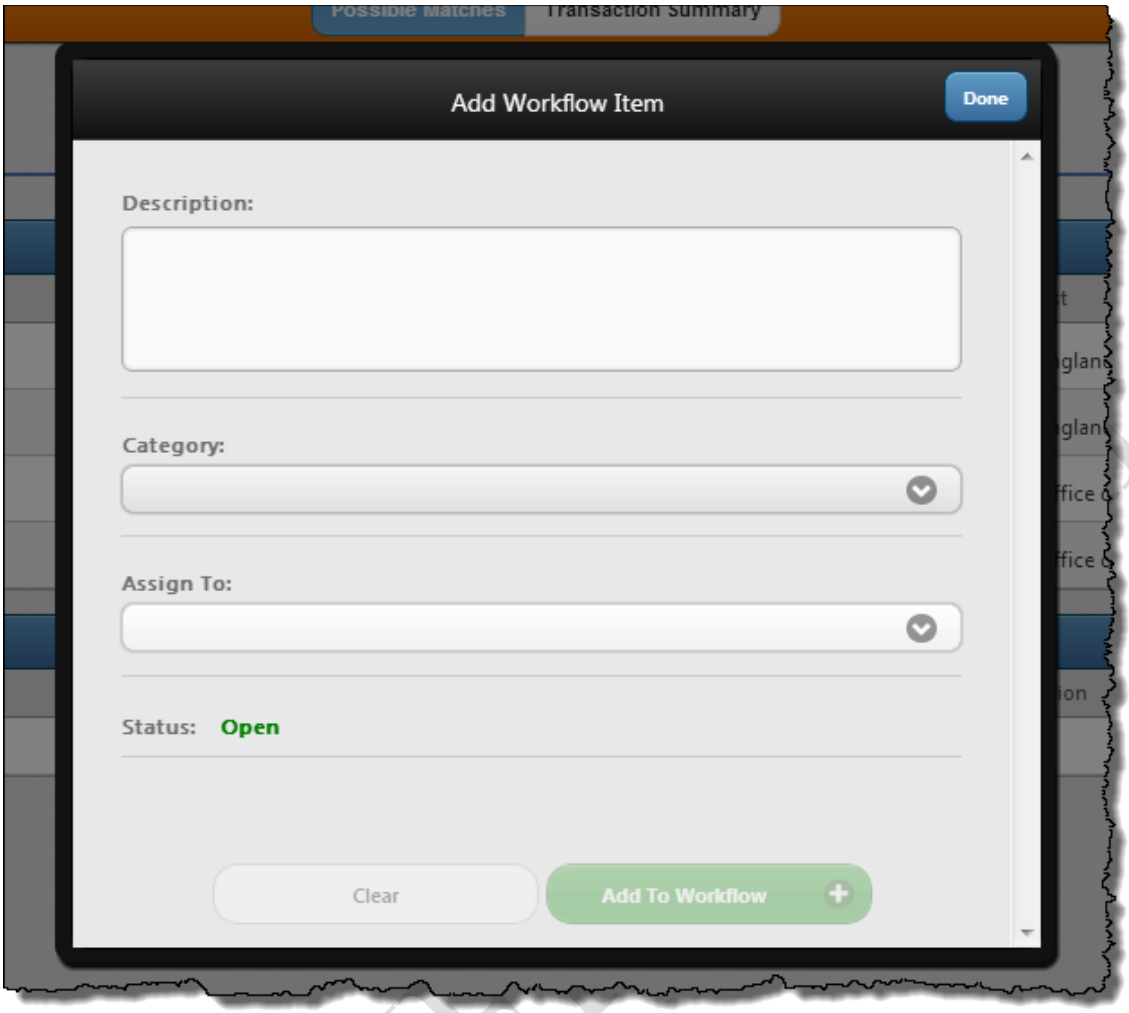
CONFIDENTIAL



2. Click on the drop down arrow to select the applicable output format. When selected, the report will open and from the page, the report can be printed or saved to your local network or computer. After printing or saving, close the window to return to the report window.
3. Select the **Done** button to return to the Transaction Details page.

Add the matched item as a Workflow Item

1. From the Options menu, select **Add To Workflow**. The Add Workflow Item window will appear.

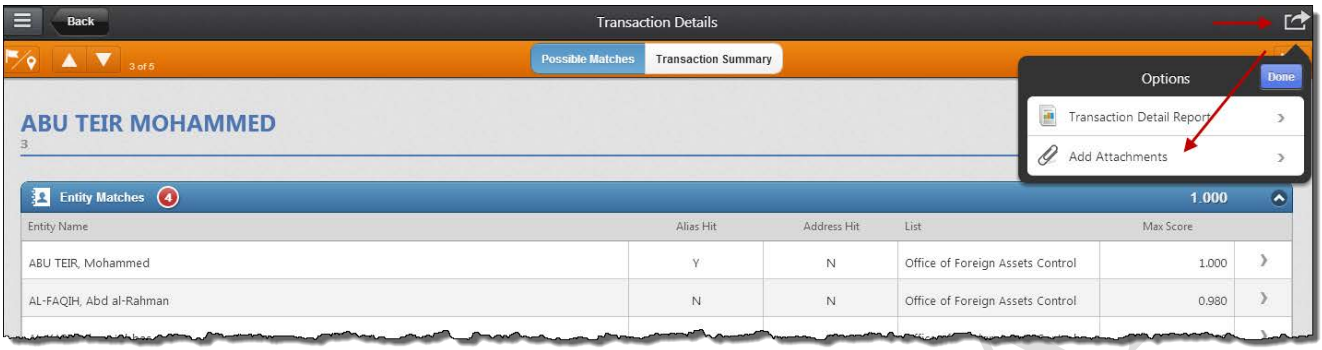


2. In the Description field, provide information for the person receiving the workflow item.
3. Select an option from the Category drop down menu.
4. From the Assign To drop down menu, select the user who will receive the workflow item.
5. Click on the **Add To Workflow** button.
6. Select the **Done** button to return to the Transaction Details page. The user, who was assigned the workflow item, will receive an email notification making them aware of the assignment.

CONFIDENTIAL

Upload an attachment

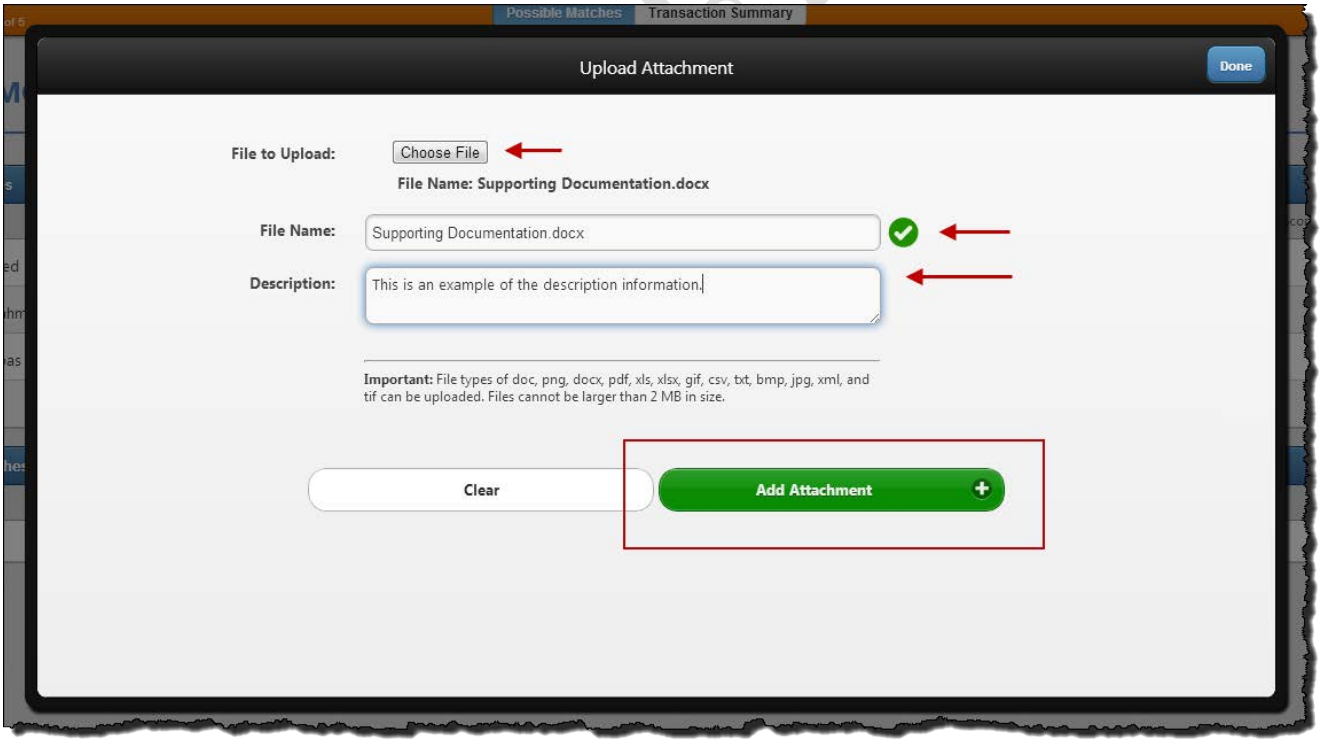
From the Transaction Details page, a document may be uploaded as an attachment. Following are a list of guidelines for uploading attachments.



- Only one document may be uploaded at one time
- Valid file formats to upload are: csv, doc, docx, txt, xls, xml, xlsx, pdf, bmp, jpg, tif, gif, and png
- Each file uploaded cannot exceed 2MB.

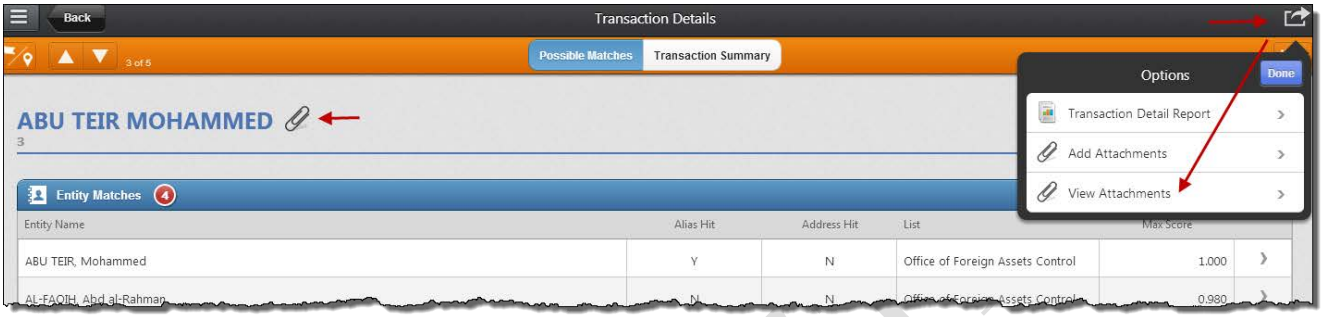
Follow these steps to upload an attachment:

1. From the Options menu of the Transaction Details page, select **Add Attachments**. The Upload Attachment window will be displayed.


Possible Matches
Transaction Summary
Upload Attachment
Done
File to Upload:
Choose File
File Name: Supporting Documentation.docx
File Name:
Supporting Documentation.docx
Description:
This is an example of the description information.
Important: File types of doc, png, docx, pdf, xls, xlsx, gif, csv, txt, bmp, jpg, xml, and tif can be uploaded. Files cannot be larger than 2 MB in size.
Clear
Add Attachment

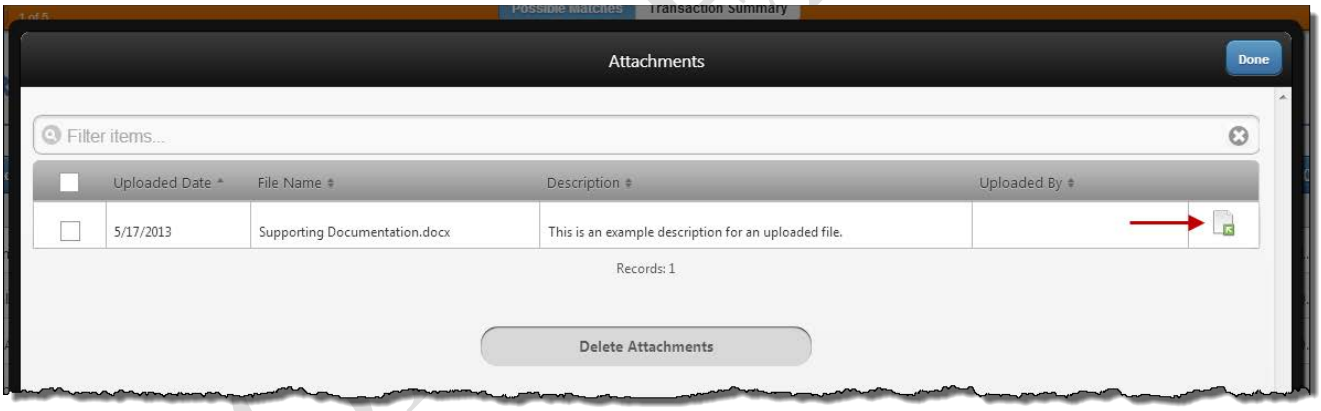
2. Select the **Choose File** button to navigate to browse and select the file to upload.
3. The File Name field will populate with the document file name. You may optionally change the file name.

4. To continue, select the **Add Attachment** button. A message indicating the file has been uploaded will be returned. The Upload Attachment window will remain open.
5. To attach another document, repeat the steps to upload an attachment.
6. Once all attachments have been uploaded, select the **Done** button. The window will close and the focus will return to the Transaction Details page.
    - An attachment icon will be displayed next to the matched item.
    - A selection to View Attachments will be included in the Options menu.



View an attachment

1. From the Transaction Details page, select the paperclip icon or from the Options menu, select **View Attachments.**

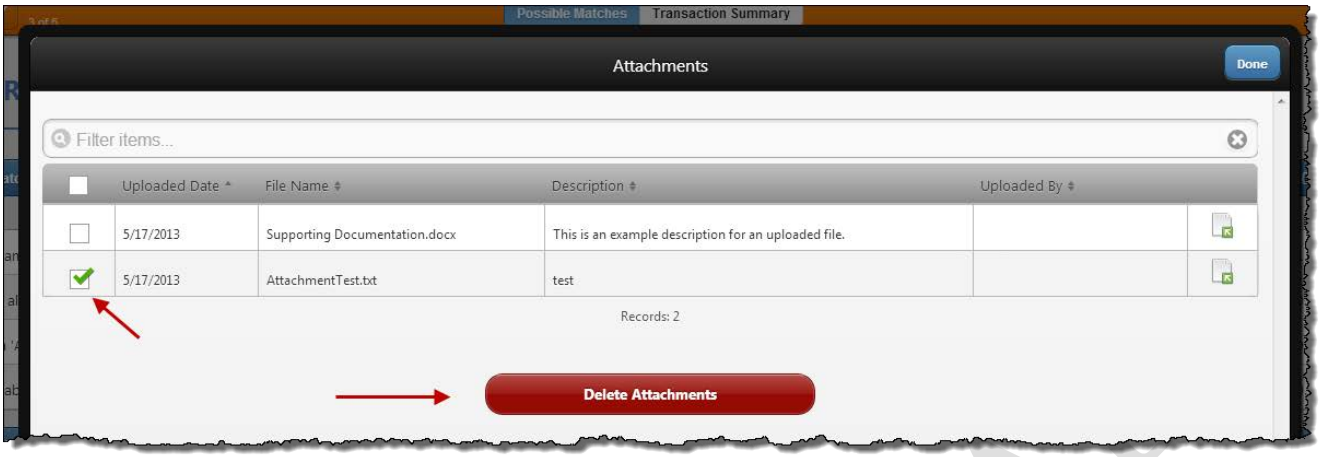


2. From the grid, select the open icon (see image above) related to the document.

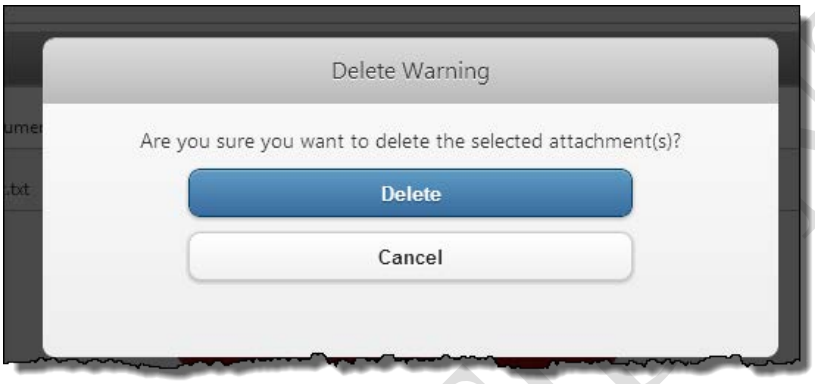
Important Note: depending on the browser, an option to open or save the file may be presented. If the file cannot be rendered to the window, then an option to save the document will be provided. For those using Chrome as the browser, a drop down menu will be displayed in the bottom left corner where the file can selected and opened.

Delete an attachment

1. From the Transaction Details page, select either the paperclip icon or select **View Attachments** from the Options menu.



2. Select the checkbox associated to the attachment(s) that will be deleted.
3. Select the **Delete Attachments** button. A warning message will be displayed.



4. Select the **Delete** button to delete the attachment.
5. Select **Cancel** to return to the grid without deleting the attachment.

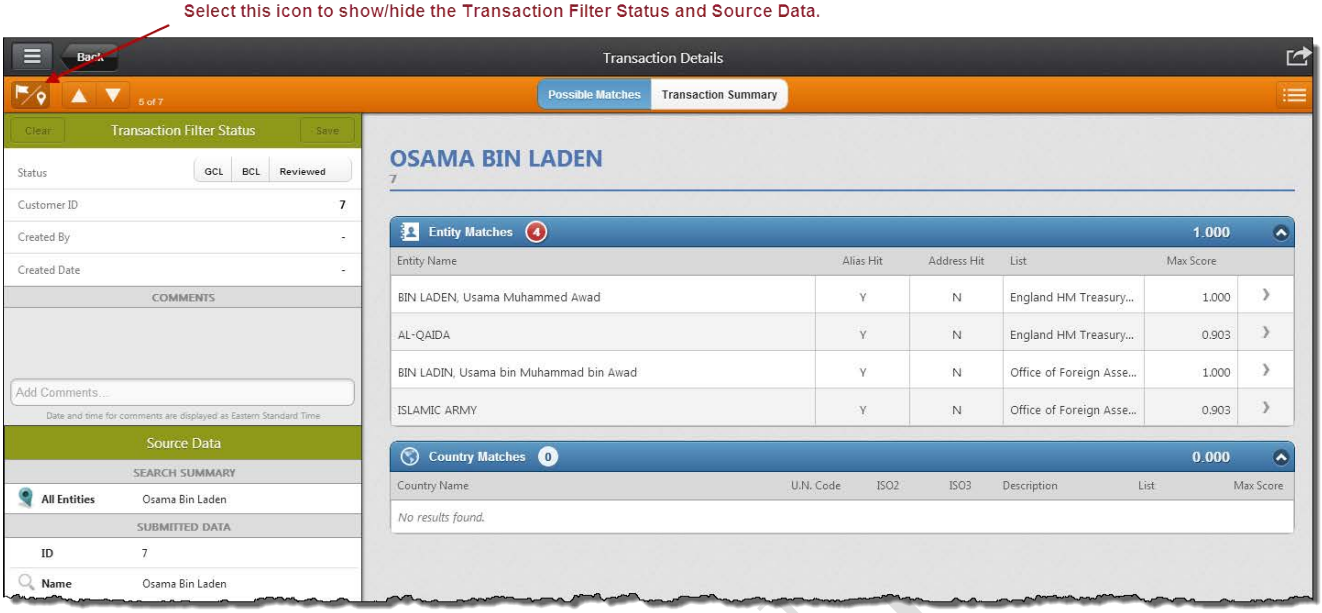
Reviewing the Transaction Filter Status and Source Data

There is an option to show/hide the transaction filter status and input source data. Here, the user can compare the input (source) data to the watch list entity data to determine a true or false positive match. Then, the Transaction Filter Status section provides the options to assign the matched item to the GCL, BCL or Reviewed status and add comments to indicate why this is a false positive or true match. When saved, the information is retained with the transaction.

Important Note: Exact ID Matching on the SSA DMF and NPI NPPES registry do not include the capability to GCL, BCL, or add comments and dispositions. Since these are exact matches only, it is not necessary to determine a false positive match based on a possible threshold of matching entity data.

- The Source Data is divided into two sections: Search Summary and Submitted Data.
- The Search Summary lists the fields that were input for single lookups and fields that were mapped for batches.
- The Submitted Data lists all the data that was submitted for screening, whether it was searched or not.

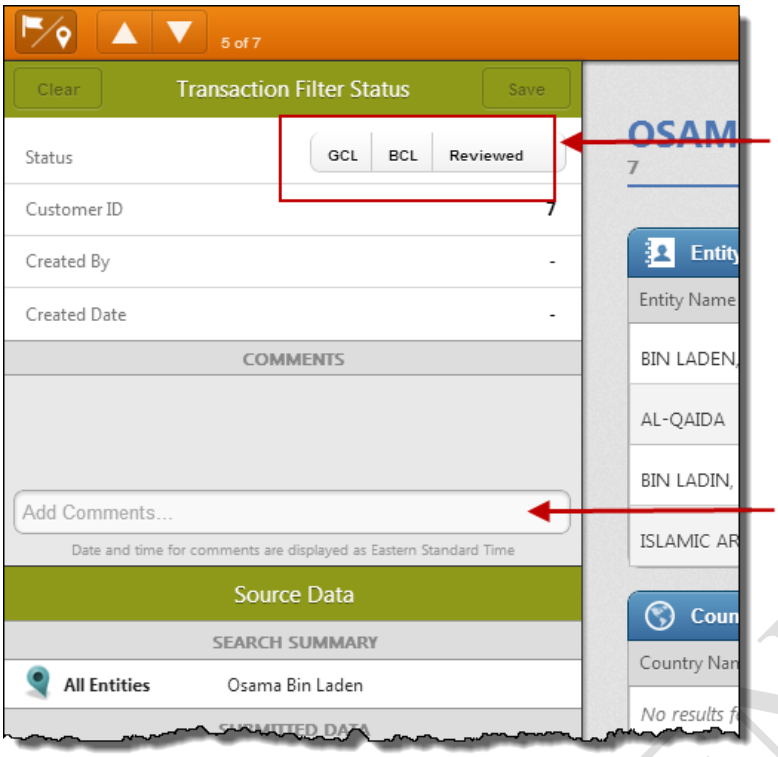
CONFIDENTIAL



Steps to assign a matched item to the GCL, BCL or Reviewed Status

1. Select the icon to show/hide the Transaction Filter Status and Source Data.
2. Optionally, enter comments in the Add Comments box (only applicable to non-Exact ID Match searches).
3. Select the **GCL, BCL or Reviewed** status button (GCL and BCL only applicable to non-Exact ID Match searches).
4. Click on the **Save** button.

CONFIDENTIAL



Input items added to the GCL and BCL will not show up as new matches in subsequent screenings unless the search threshold is reduced or additional items are added to the watch list entity where originally matched.

Important Note: If your institution performs single item screening via web service and a unique id is supplied with the request, the customer can be assigned the GCL or BCL filter status. Items are screened via the Screen a Single Item cannot be added to the GCL/BCL.

CONFIDENTIAL

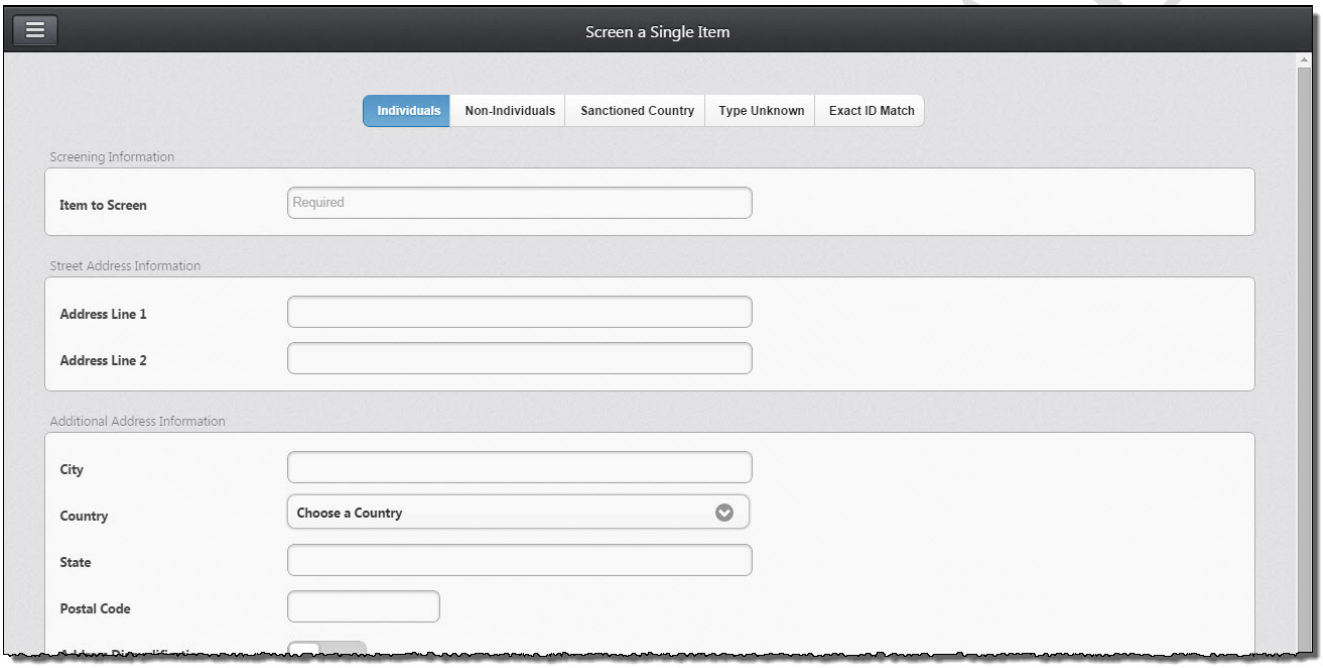
Screen a Single Item Overview

WatchDOG Elite provides the capability to screen against individual and non-individual entities via the Screen a Single Item feature. From these pages, you can screen customer information against a variety of watch lists. In addition, there is an option to screen a sanctioned country against OFAC's sanctioned countries list and an option to complete an exact ID search on Social Security Numbers against the Death Master File (DMF) or search National Provider Identifiers against the National Plan & Provider Enumeration System (NPPES) registry.

How to screen a single item

This section provides the instructions on screening a single item via the user interface.

1. From the Navigation toolbar, select **Screen a Single Item**. The Screen a Single Item page will display.



See the following information for detailed instructions on entering search criteria.

- The fields are not case sensitive. You may use upper or lower case or both.
- The fields accept both alpha and numeric characters.
- The order of items does not matter; Last/First or First/Last each provides the same results.
- You may use special characters, such as hyphens, periods, apostrophes, etc.

2. Select the search method of Individual, Non-Individual, Country, Type Unknown, or Exact ID Match. In the example and steps below, the **Individual** link is selected.
3. If applicable, select a division to associate the customer name.
4. Optionally enter the Street Address information and other elements of the address.

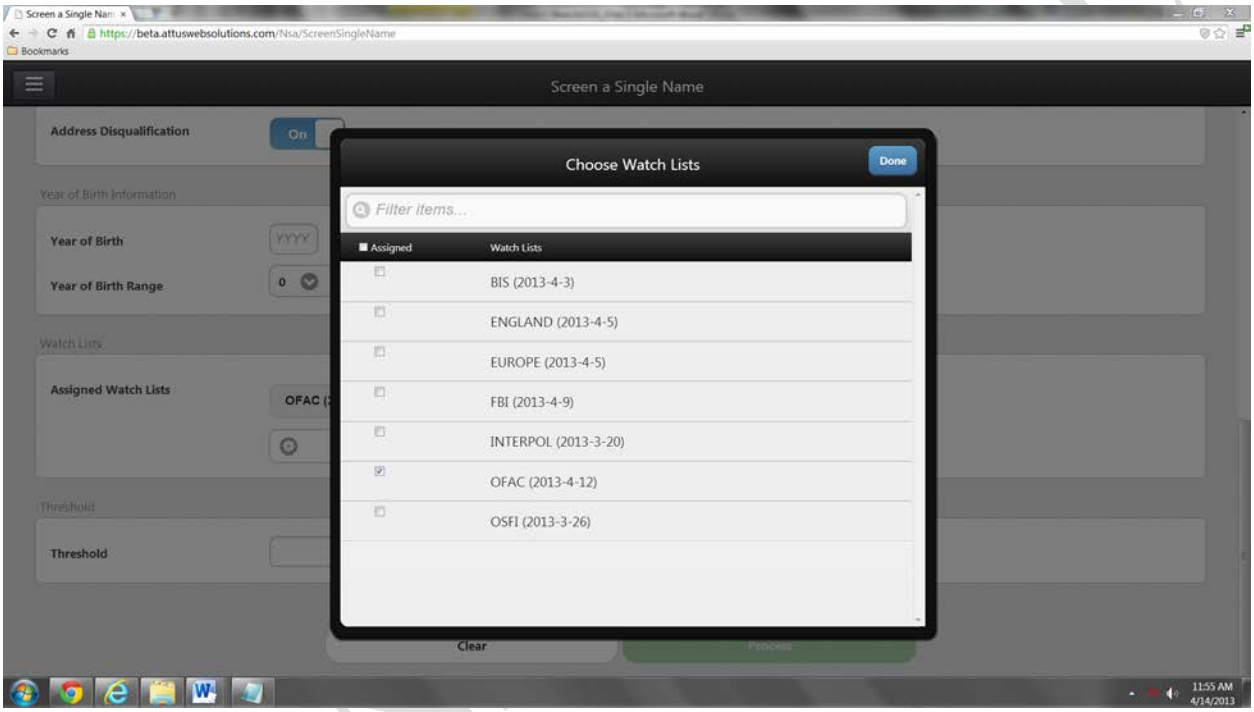
   Important Note: If a Street Address is provided, the system will screen both the name and the address against the selected watch lists. If other elements of the address (such as the city, state, zip) are provided, these will be included in the matching/disqualification process.

5. Set the Address Disqualification option to **Yes/No**.

   If your search includes an OFAC sanctioned Country, the hit results indicate that the country is sanctioned. For example, if you search on Osama bin Laden AND Cuba, the hit results will show that Cuba is sanctioned where the link to OFAC's Sanctioned Countries list will display.

6. Optionally enter DOB Year (or your best guess) using 4 numbers. Select the DOB Range (0 to 5) from the drop down list. For example, if the DOB is 1955, and the range is "2", the algorithm searches all dates from 1953 to 1957.

7. In Watch Lists section, click on the **Edit Watch Lists** button. Then, select the applicable watch lists. After selecting the lists, click on **Done**. The window will close and return you to the Screen a Single Item page.



8. Optionally, change the Threshold. The valid values are from .80 to 1.00 (80% to 100%).

9. Click **Process** to begin the search and match process.

Screening a Sanctioned Country

To screen a country, use the **Sanctioned Country** link.

Sanctioned Country searches are performed against the OFAC and FATF lists only.

1. From the Screen a Single Item page, select the **Sanctioned Country** tab.

2. If applicable, select a division in which to associate the search.

3. In Watch Lists, check the **OFAC** watch list.

4. Click **Process** to begin the search and match process.

   Important Note: If the screening results in a possible match, a red indicator will be visible in the Country Matches section of the Transaction Details page (the screening results). In addition, an external link to

the watch list source will be provided. Please see the image below for an example of a possible sanctioned country match.

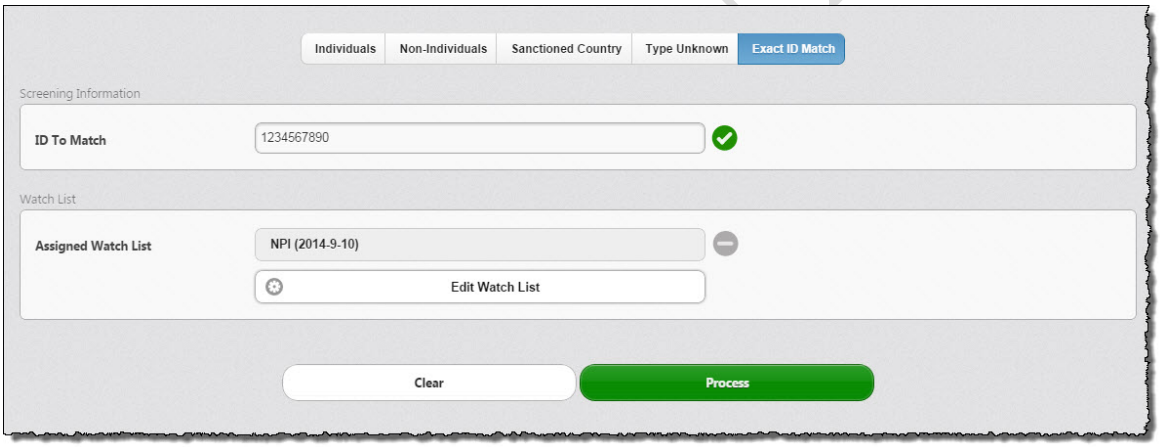
Screening an Exact ID Match

The Exact ID Match option allows the user to either search for expired Social Security Numbers against the Social Security Administration (SSA) Death Master File (DMF) or search for valid National Provider Identifiers against the National Plan & Provider Enumeration System (NPPES) registry.

The Exact ID Match feature is optional and will only be visible if the Function for this type of searching has been enabled for the user. If enabled, the Exact ID Match option will appear as a tab on the Screen a Single Item screen.

1. From the Screen a Single Item page, select the **Exact ID Match** tab.
2. Enter the exact ID to match.
3. In Watch Lists, select the **Edit Watch List** button to select the correct list to match against.

   Important Note: Because this is an exact match search on a specific identifier, SSN or NPI, which will only be listed on the corresponding list you can only search one list at a time, either the DMF or the NPI registry. Make sure you have selected the correct list that corresponds with the type of ID you are entering.



4. Click **Process** to begin the search and match process.

Reviewing the results of the single item screening

See Transaction Details Overview on page 12 to learn about the review and resolve process and adding the matched item to the GCL, BCL or Reviewed filter.

CONFIDENTIAL

Screen a Batch File Overview

This section details the steps in which to submit a customer batch file for screening via the user interface.

Important Note: If your institution submits batches via ftp, you will be provided a separate document.

Steps to submit a batch file for screening

1. From the Navigation toolbar, select **Screen a Batch File**.
2. In **Source and Layouts,** complete the fields as follows.

   Batch Settings: Select a setting from the drop down list of saved settings. To add a new setting to the list, select the plus sign; this opens a blank New Setting Name field. Enter the new batch setting. (When you process the batch, the new setting name is placed in the drop down list).

   Important Note: To create a new setting, the user must have the Batch Override Settings function assigned.

   Batch Source: Select the **Choose File** button to Windows dialog box; select your customer data file and click **Open**. This places the file name in the Batch Source text box.

   Batch Name: Optionally enter a batch name.

   File Layout: Select the format that matches your customer data file.

   Contains Header: If the input data file contains a header row select this option. If checked, the header row column names will be provided in the field mapping section. Please note that default column names will appear if you either 1) do not have a column header in your data file, or 2) you do NOT select the Contains Header checkbox. This will be reviewed in the next section.

3. Select the **Edit Field Mapping** button to map the input data fields to the system equivalent mapping.

   Guidelines for the Field Mapping Process

   Here are some basic guidelines for mapping the fields in customer data file.

Field Name	Description	How to Map	
		Map this field in your customer data file . . .	To the data type in the Field Mapping Column. . . .
Individual	Person	Full name in a single field	"Full Name"
		First and Last name in separate fields	Map the first name to "First Name" and last name to "Last Name"
Non-individual	Entity, such as a business, corporation, vessel, etc.	Non-individual	"Non-Individual"
Both	Individuals or non-individuals	Both individual and non-individual	"All Entities"
Account*	Excludes items	Account or other	"Account Number.

CONFIDENTIAL

*Required for GCL and BCL	flagged as 1) good customers, or 2) or blocked customers.	identifying number	Unique Identifier"
Address	Address, including street, city, state, postal code, and/or country.	Street Address	"Address"
		City	"City"
		State	"State"
		Postal Code (Zip)	"Postal Code"
		Country	"Country"

4. **Batch Selections**: This section displays the last saved settings.

   Threshold: Accept the default threshold or enter a new one (it is recommended to begin the threshold at .85 and test the number of hits. If necessary, increase the threshold to reduce the number of false/positives.).

   Address Disqualification: Select if you want to use addresses to disqualify items from appearing in your matched items.

   Important Note: In order to use address disqualification, each element of the address such as city, state, postal code and country must be in a separate column (or cell).

   Search Street Address: If checked, the system will search where the name OR street address matches. The user is allowed to optionally select the batch to include the street address search.

   Year of Birth Disqualification: Select if you want to use date-of-birth to disqualify names from appearing in your matched names.

   Important Note: In order to use DOB disqualification, the date-of-birth field must be mapped.

   Batch Notification: Select to use the email notification (as set up in Configuration). Setting to On enables the Notification Settings section.

   Notification Settings: Optionally select predefined email groups to receive a notification upon completion of the batch processing.

5. In Watch Lists, select the **Edit Watch Lists** button to assign the applicable list(s) you want to use for matching against your customer data file.
6. Click **Save** to retain your new settings.
7. **Process:** Submits the batch file if you have saved the field mappings.

   Note: If you are using a custom layout, you may skip the field mapping page and click on the Process button.

8. When the Process button is selected, a Batch Submit Summary box will be displayed with a brief batch summary and options to go to the Review Batch File Results page or to Screen a Batch File. Select the applicable option.

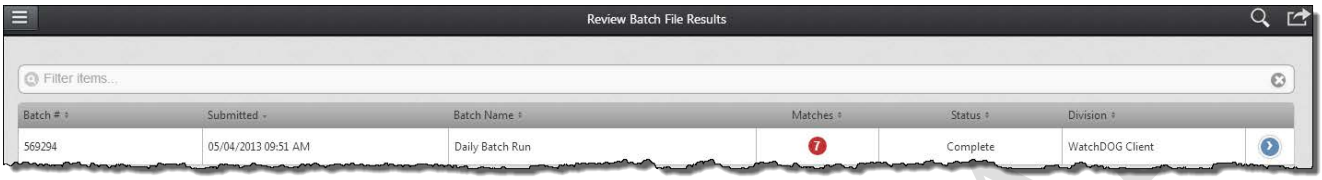
CONFIDENTIAL

Review Batch File Results

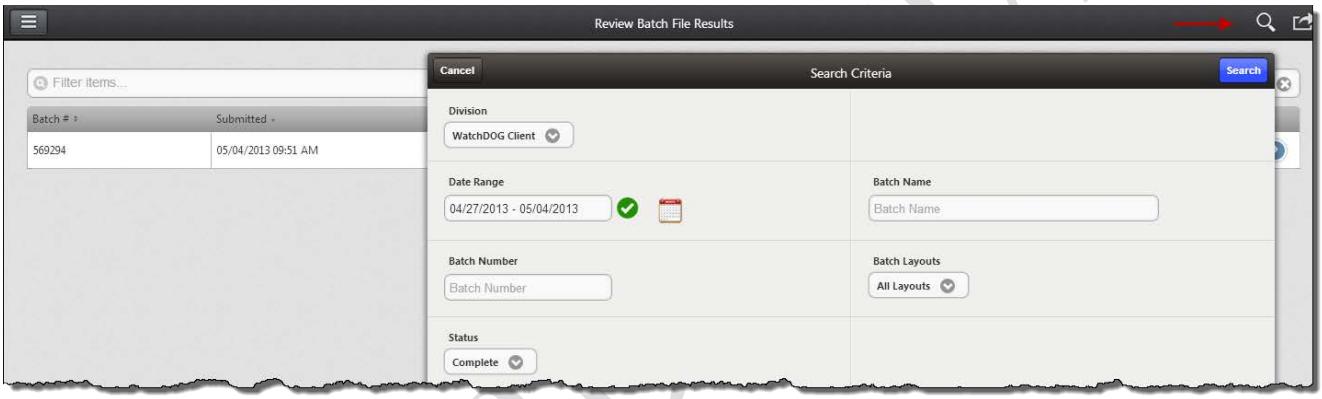
Users with access to this page can retrieve and manage the results of screened batches and review several batch related reports.

Steps to search and retrieve completed batch results

1. From the Navigation toolbar, select **Review Batch File Results**. The grid will load with any results based on the default search criteria.



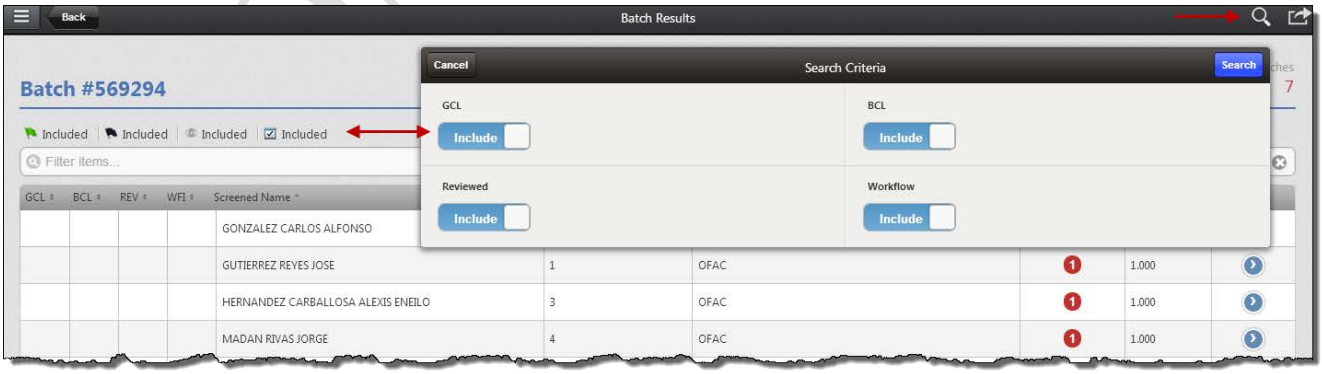
If the applicable batch is not in the list, the search criteria may be modified by clicking on the Search icon.



2. Upon modifying the search criteria, select the **Search** button. Results based on the criteria will be displayed in the Review Batch File Results grid.

   In addition to the Search Criteria field, particular data can be searched via the Inline Filter search bar.

3. From the Review Batch File Results grid, click one the row applicable to the results. The Batch Results page will load with the matched items.



The results set are returned based on the defined search criteria. In the above example, the search settings are defined to show in the results set the matched items that have already been GCL/BCL in this batch or a previously scanned batch. In addition, there are options to include/exclude Reviewed and Workflow items from the list.

Reviewing the results of a single item screening

See Transaction Details Overview on page 12 to learn about the review and resolve process and adding the matched item to the GCL, BCL or Reviewed filter.

Batch Options

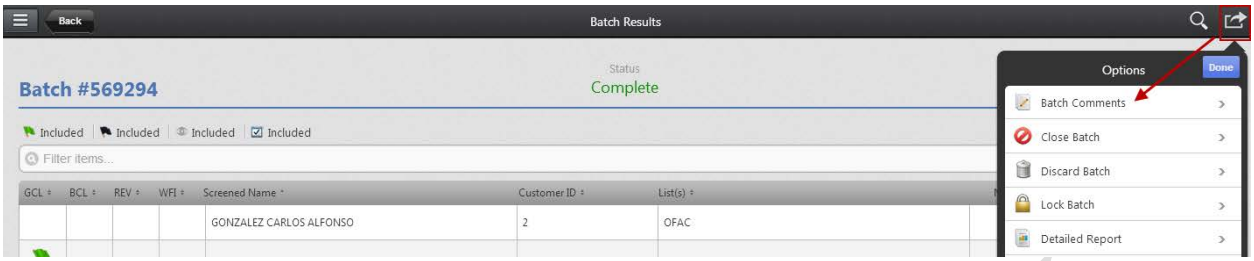
The batch Options menu consists of various batch functions and reports. In this section, we will review the following:

- Batch Comments – used to optionally save remarks related to the entire batch.
- Close Batch – optionally set the status of the batch to Closed, upon completion of the review and resolve process.
- Discard Batch – optionally use this status if the batch was incorrectly sent or there were problems processing the batch.
- Lock Batch – optionally use this status to prevent other users from saving data to the batch while one user has it opened.
- Add To Workflow – the entire batch or one transaction may be assigned as a workflow item to another user of the system for review.

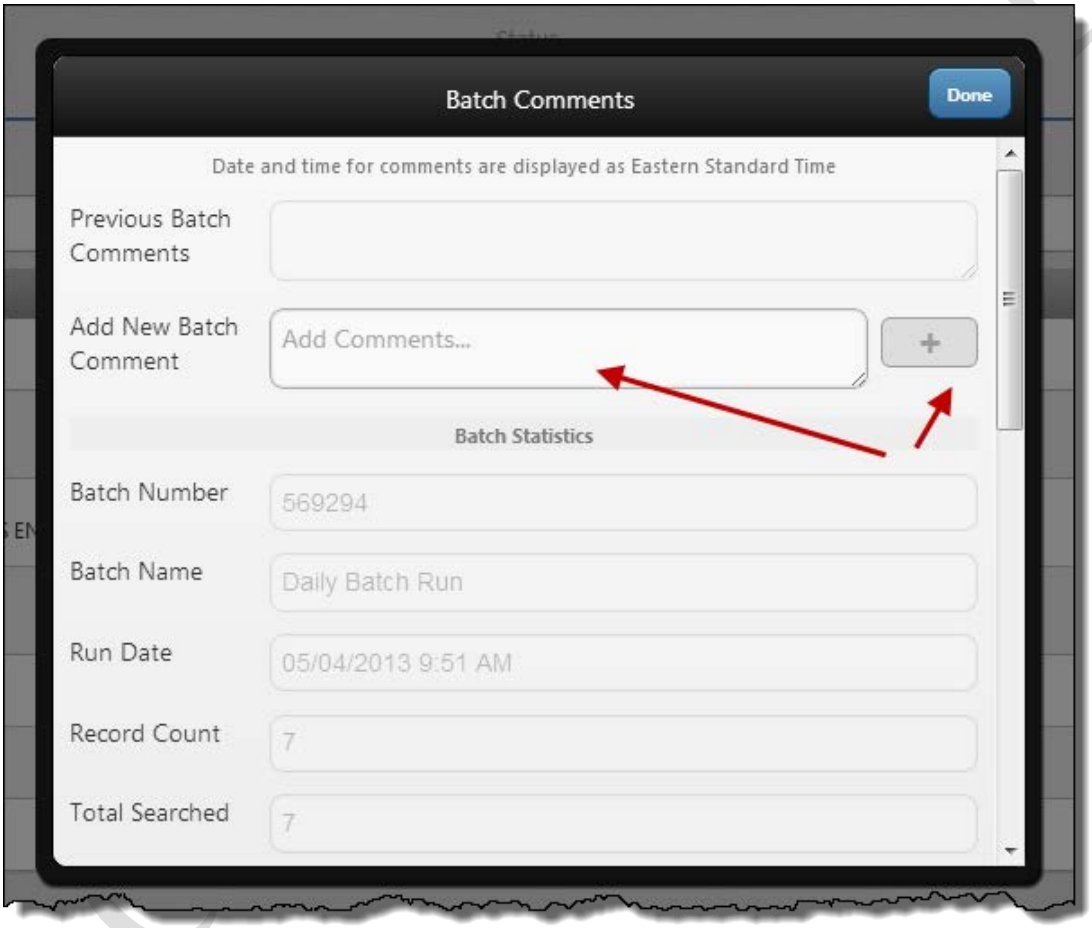
CONFIDENTIAL

Steps to add Batch Comments

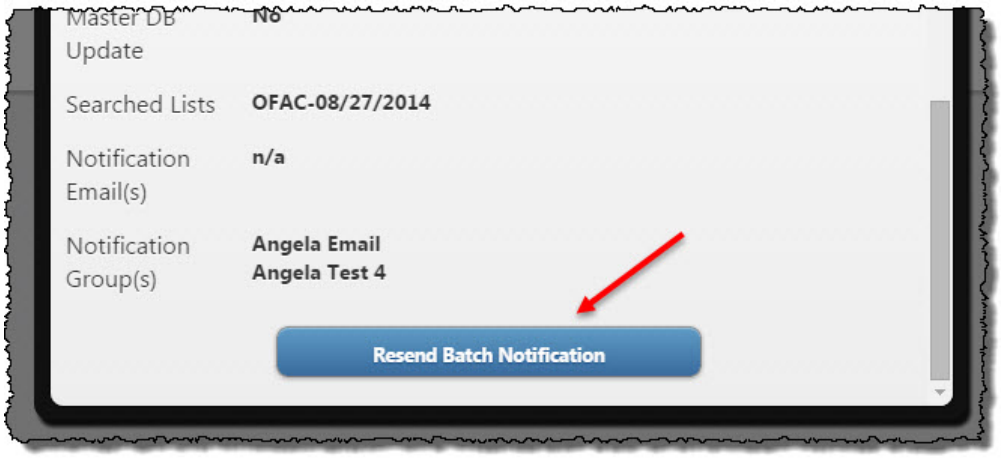
1. From the Options menu of the Batch Results page, select **Batch Comments**.



The batch comments, along with the batch statistics, will be opened in a separate window.



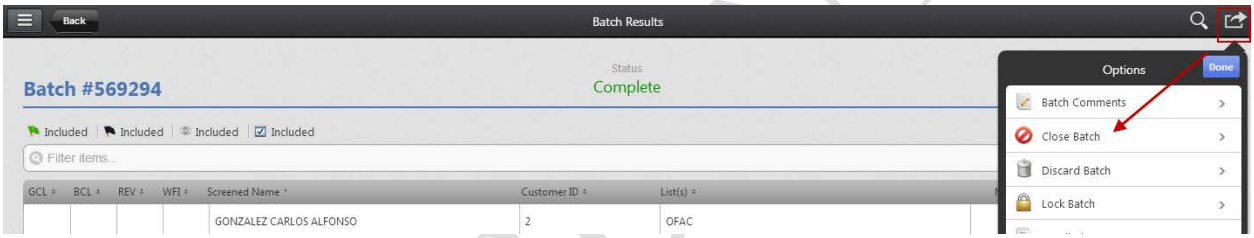
2. In the Add New Batch Comments box, provide any remarks and click the **Done** button to return to the Batch Results page.
3. From the Batch Comments pop-up window, you can also choose to Resend the Batch Notification to the original recipients.



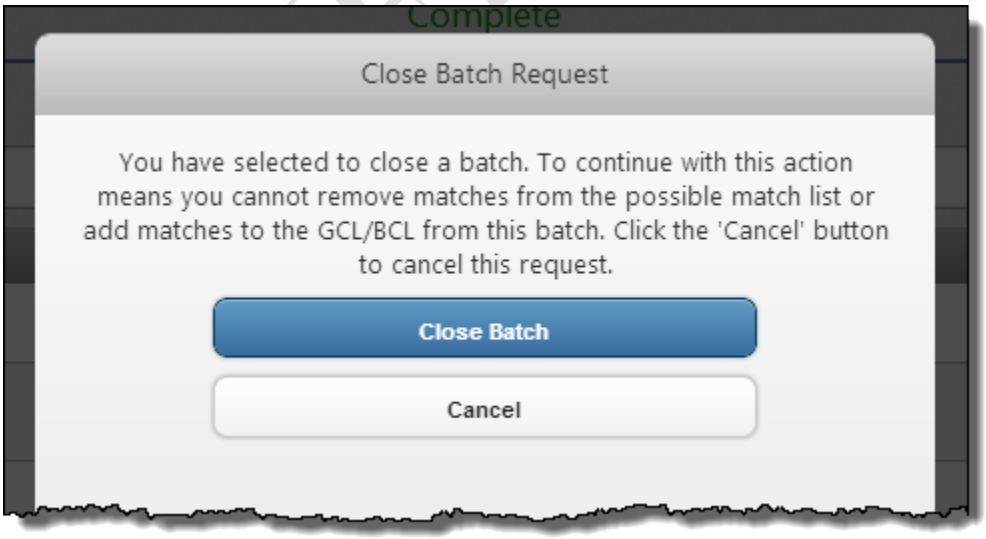
Scroll to the bottom of the Batch Comments pop-up and select the **Resend Batch Notification** button. A copy of the original email will be sent to the original recipients.

Steps to Close a Batch

1. From the Options menu of the Batch Results page, select **Close Batch**.



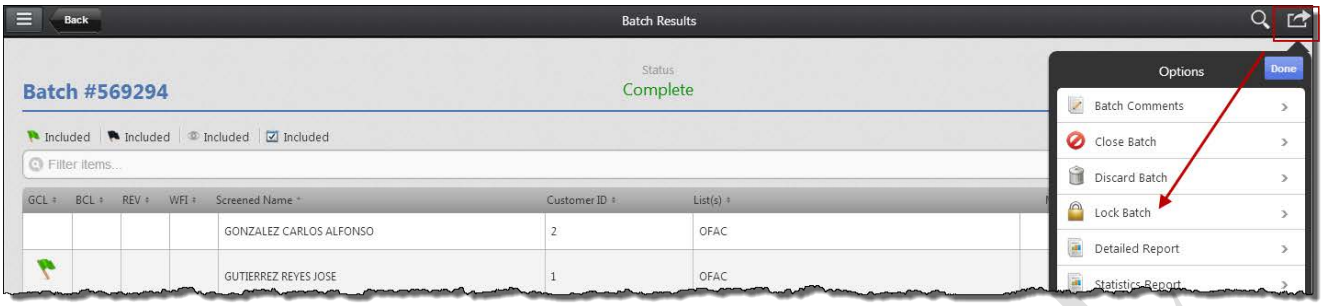
The confirmation box will be opened in a separate window. There are options to either continue with the closing of the batch or to cancel the action.


Complete
Close Batch Request
You have selected to close a batch. To continue with this action means you cannot remove matches from the possible match list or add matches to the GCL/BCL from this batch. Click the 'Cancel' button to cancel this request.
Close Batch
Cancel

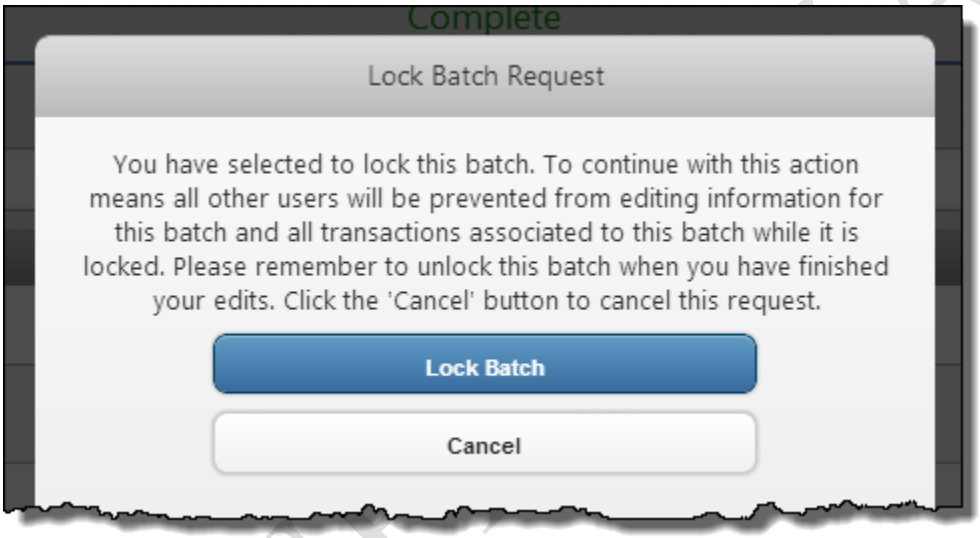
2. Select **Close Batch** to continue with the action; the focus will remain on the Batch Results. Select **Cancel** to remain on the Batch Results page without closing the batch.

Steps to Lock a Batch

1. From the Options menu of the Batch Results page, select **Lock Batch**.

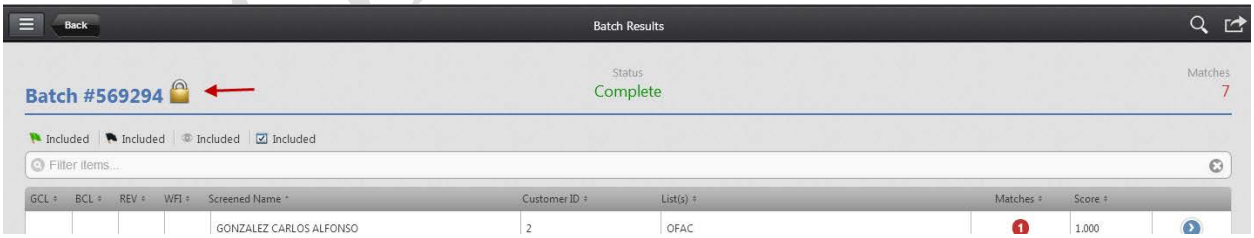


The confirmation box will be opened in a separate window. There are options to either continue with the locking of the batch or to cancel the action.


Complete
Lock Batch Request
You have selected to lock this batch. To continue with this action means all other users will be prevented from editing information for this batch and all transactions associated to this batch while it is locked. Please remember to unlock this batch when you have finished your edits. Click the 'Cancel' button to cancel this request.
Lock Batch
Cancel

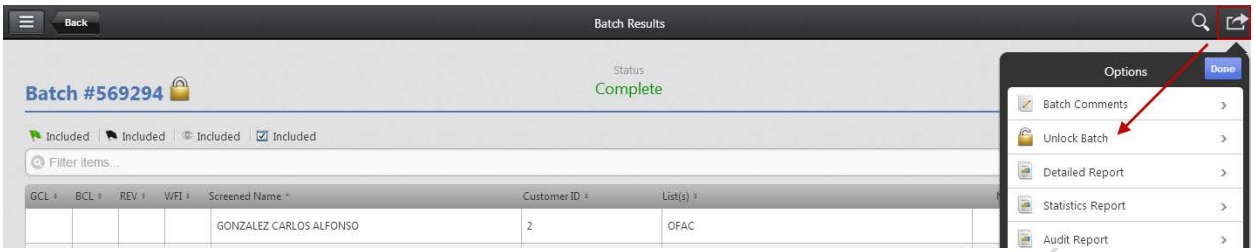
2. Select **Lock Batch** to continue with the action and return to the Batch Results grid or Cancel to remain on the Batch Results page without locking the batch.

   When a batch is locked, an icon will be displayed next to the batch number.



Steps to Unlock a Batch

1. From the Options menu of the Batch Results page, select **Unlock Batch**. The batch is now unlocked.



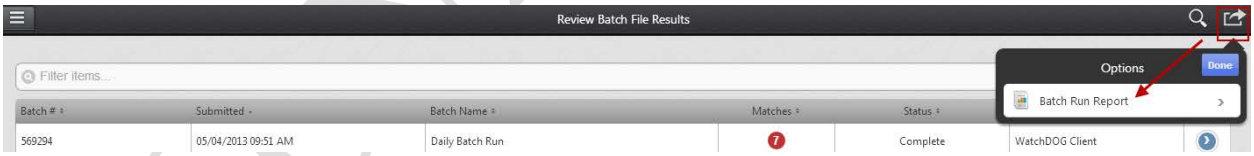
Batch Reports

Based on your access level, several reports are available from the Review Batch File Results and Batch Results pages. Let's look at each one separately. The available reports are as follows:

- Batch Run Report - The purpose of this report is to gather the current status of a batch(es) based on watch lists scanned and items filtered by GCL/BCL/Removed/None.
- Detailed Report – the results set for the report contains the search attributes, the input source data and the watch list entity information. In addition, the matched items are indicated with the GCL/BCL/Reviewed filtering status flag as well as any saved comments.
- Statistics Report – consists of the search attributes such as threshold and watch lists screened against as well as any saved batch comments.
- Audit Report - Displays any matched items added to GCL, BCL or Reviewed for the batch. The date and user who added the item is provided as well as the lists hit against.

Steps to run the Batch Run Report

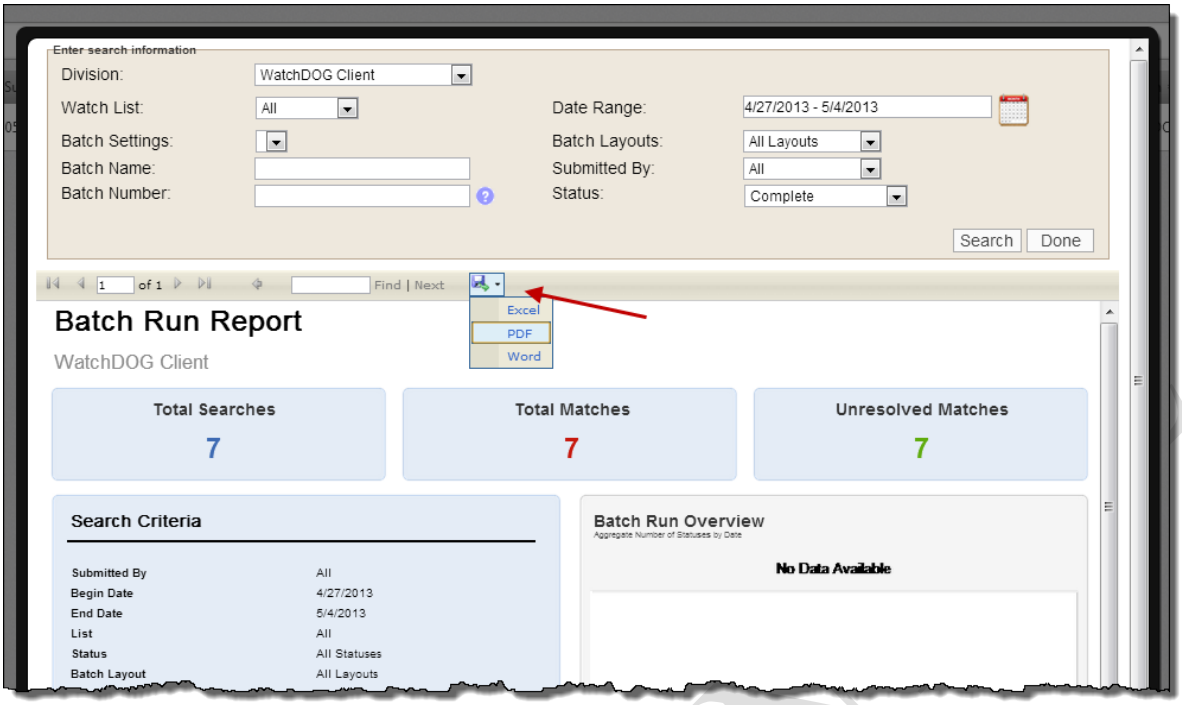
1. From the Options menu of the Review Batch File Results page, select **Batch Run Report**.



The results will be opened in a separate window.

2. To print/export the report, click on the applicable option from the drop down menu.

CONFIDENTIAL

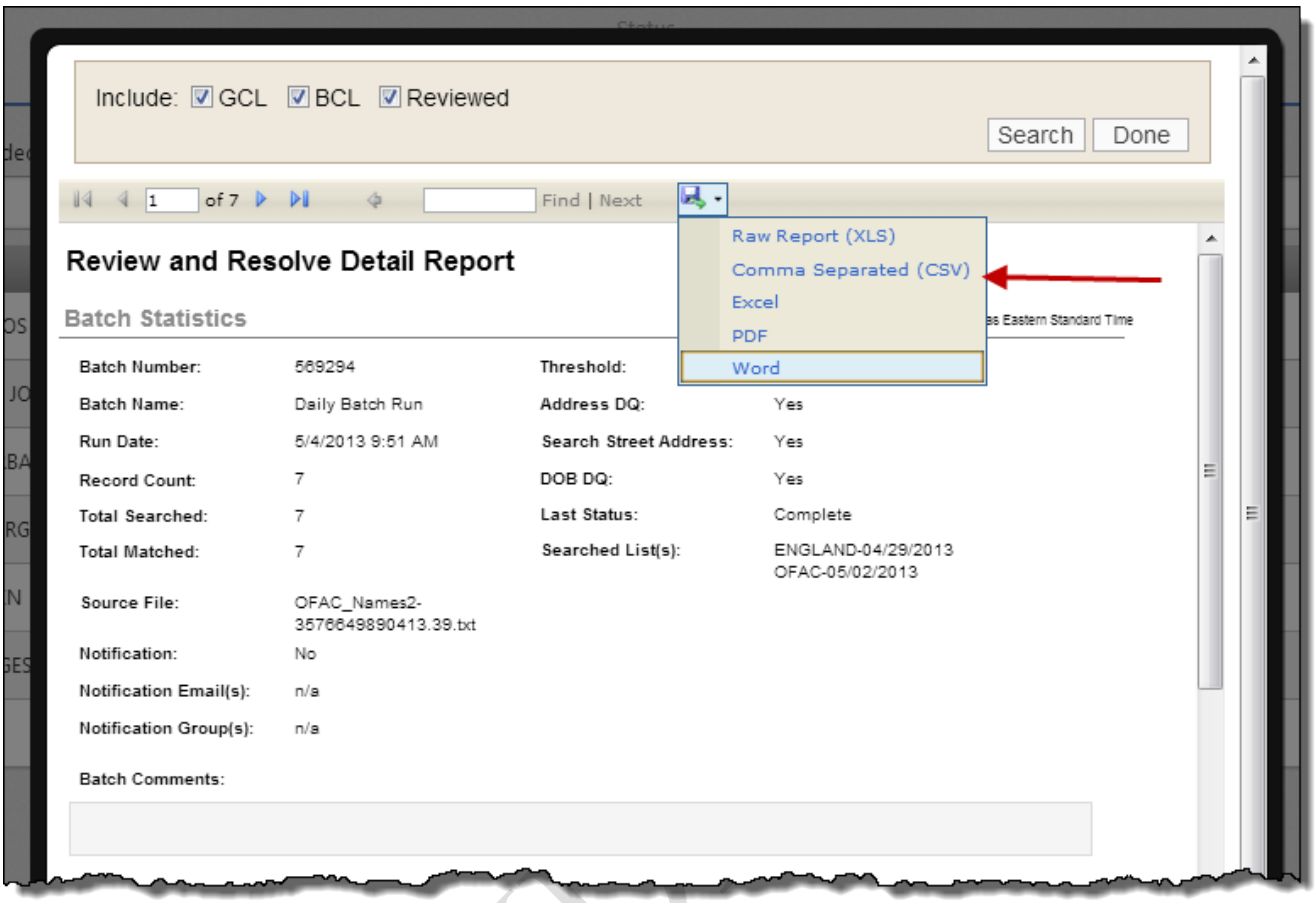


3. To modify the results set, use the search fields on this page to modify the criteria and click the **Search** button.
4. When completed with print/export, click the **Done** button to close this page and return to the Review Batch File Results page.

Steps to run the Detailed (Batch) Report

1. From the Options menu of the Batch Results page, select **Detailed Report**. The results will be opened in a separate window.
2. By default, the GCL/BCL/Reviewed items are included in the results set. To remove the items from the report, select the applicable options and click the **Search** button. The new results set will load in this same window.
3. To print/export the report, click on the applicable option from the drop down menu.

CONFIDEN

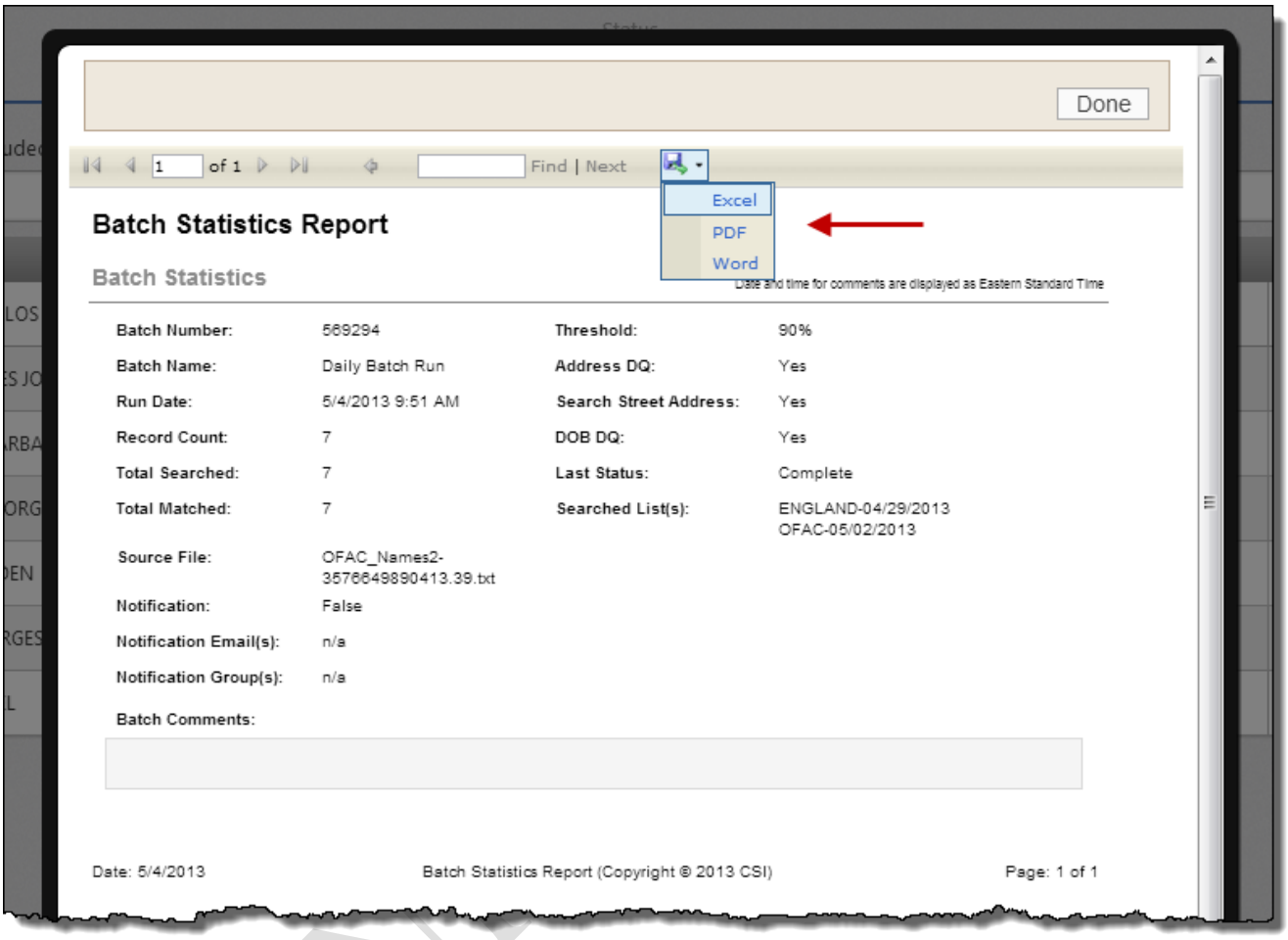


4. When completed with print/export, click the **Done** button to close this page and return to the Batch Results page.

CONFID

Steps to run the Statistics Report

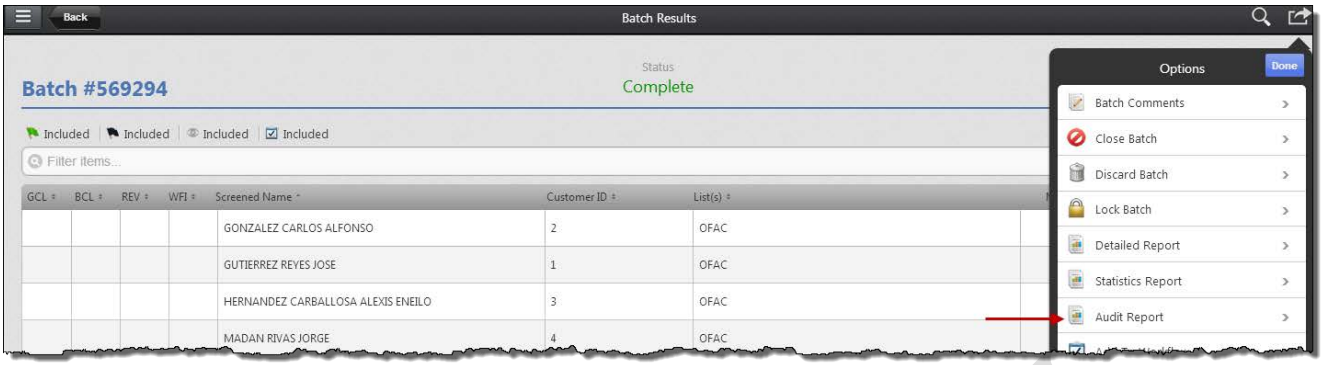
1. From the Options menu of the Batch Results page, select **Statistics Report**. The results will be opened in a separate window.



2. To print/export the report, click on the applicable option from the drop down menu.
3. When completed with print/export, click the **Done** button to close this page and return to the Batch Results page.

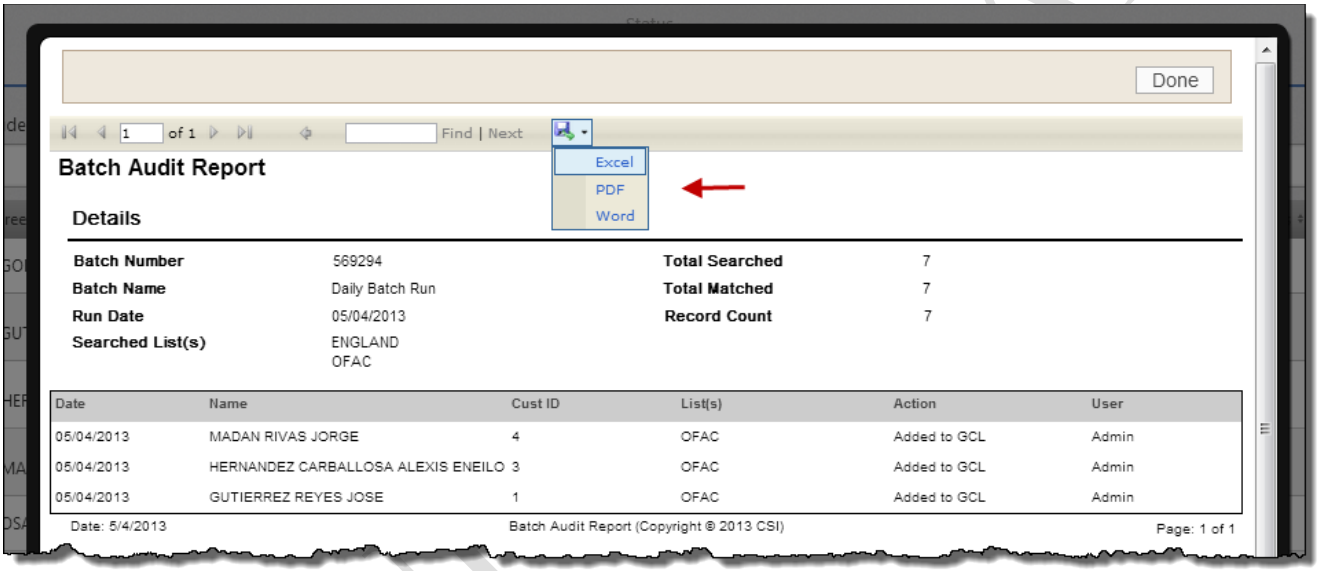
Steps to run the Audit Report

1. From the Options menu of the Batch Results page, select **Audit Report**.



The results will be opened in a separate window.

2. To print/export the report, click on the applicable option from the drop down menu.


Done
1 of 1
Find | Next
Excel
PDF
Word
Batch Audit Report
Details
Batch Number 569294
Batch Name Daily Batch Run
Run Date 05/04/2013
Searched List(s) ENGLAND OFAC
Total Searched 7
Total Matched 7
Record Count 7
Date Name Cust ID List(s) Action User
05/04/2013 MADAN RIVAS JORGE 4 OFAC Added to GCL Admin
05/04/2013 HERNANDEZ CARBALLOSA ALEXIS ENEILO 3 OFAC Added to GCL Admin
05/04/2013 GUTIERREZ REYES JOSE 1 OFAC Added to GCL Admin
Date: 5/4/2013
Batch Audit Report (Copyright © 2013 CSI)
Page: 1 of 1

3. When completed with print/export, click the **Done** button to close this page and return to the Batch Results page.

Review Transactions Overview

This page is used to filter and retrieve previously screened items that have been performed via the user interface, automated batch submissions or web services.

Important Note: Only those items scanned via the Screen a Single Item page and web services are retained in the database as well as items scanned via a batch where a possible match is produced. If it is a requirement of your institution to store all searched items, please see your CSI Regulatory Compliance representative to inquire about the Customer Master feature.

Steps to search for a previously screened item

1. From the Navigation toolbar, select the **Review Transaction** link. Only those transactions that meet the default search criteria will be returned in the Review Transactions grid.

CONFIDENTIAL

If the transaction (screened item) IS in the grid:

2. Select the row associated to the item to open the Transaction Details page. See Transaction Details Overview on page 12 to learn more about actions to take to resolve the matched item.

If the transaction (screened item) IS NOT in the grid:

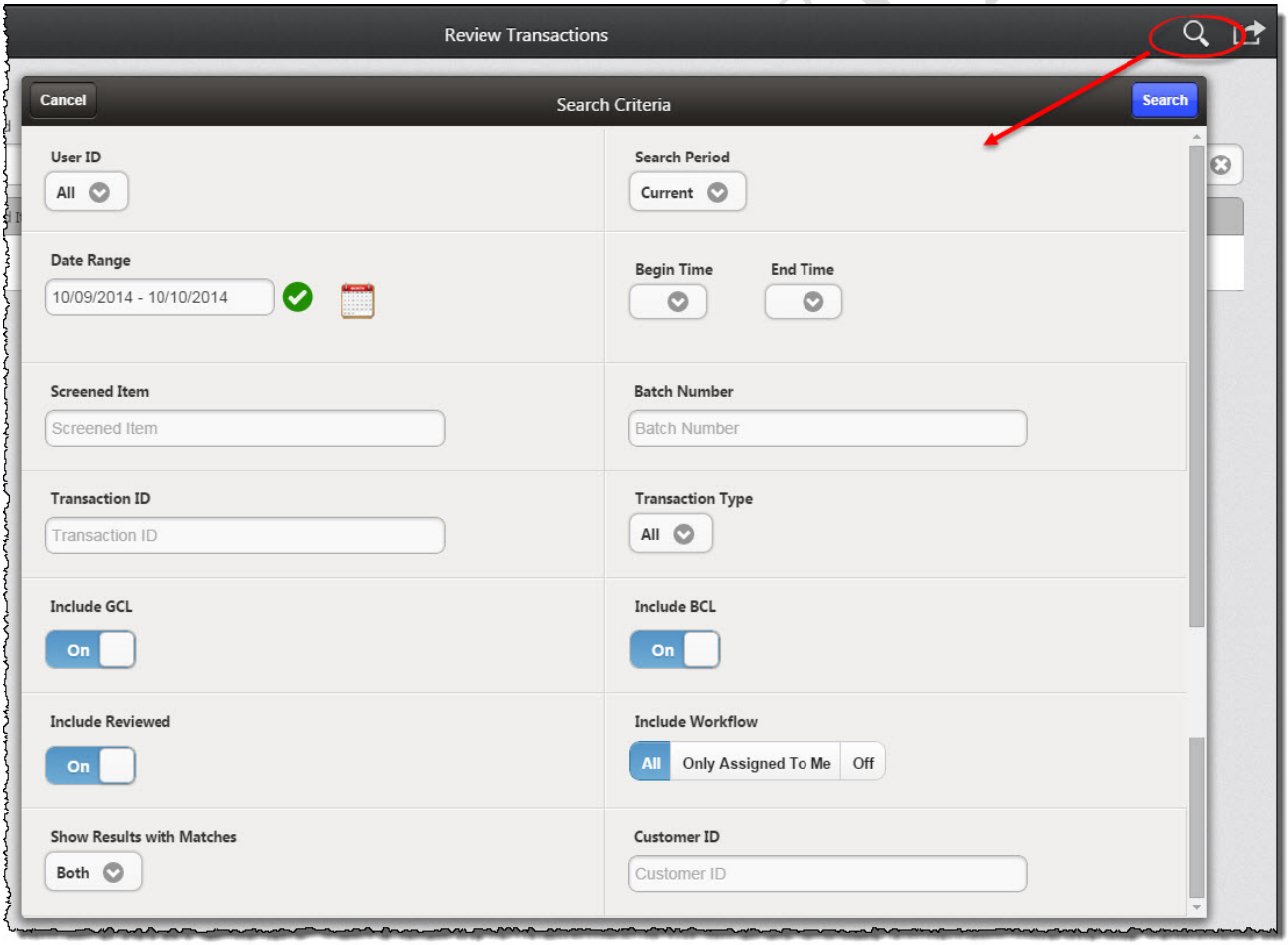
3. Select the **Search** icon and refine the search criteria in the fields you want to use for this search (you may use more than one field). By default, only one day of data is returned.

   Search Period – the options are 'Current' or 'Archived'; defaults to Current.*

   To search for data entered in the past 13 months, use **Current** and change the Start Date and End Date accordingly, if applicable.

   To search for data older than 13 months, use the **Archived** option and change the Start Date and End Date accordingly, if applicable.

4. Define any additional search criteria as desired from the available search fields.
5. Upon defining the search criteria, select the **Search** button. The results set will be displayed in the Review Transactions grid.



This completes the Watch List Screening section!

CONFIDENTIAL

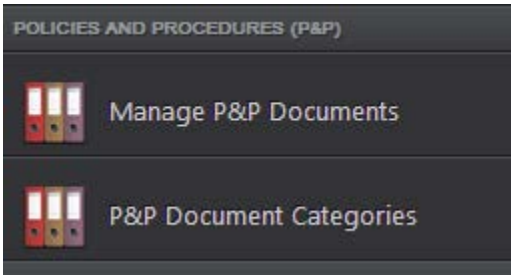
Policies and Procedures Overview

Important Note: This guide is written with the assumption that all roles and users have been defined and created within the application. Please see Chapter 9 in the full user manual, which can be accessed via the Product Documentation link in the Navigation toolbar, for a more detailed explanation of all functions and reports as well as the functions required to access the features and functionality.

Navigation:

Most of the navigation within the application is driven through the left side Navigation toolbar.

Only those links which the user has access to via security functions will be available in the Navigation toolbar. For Policies and Procedures, the section will be displayed as:

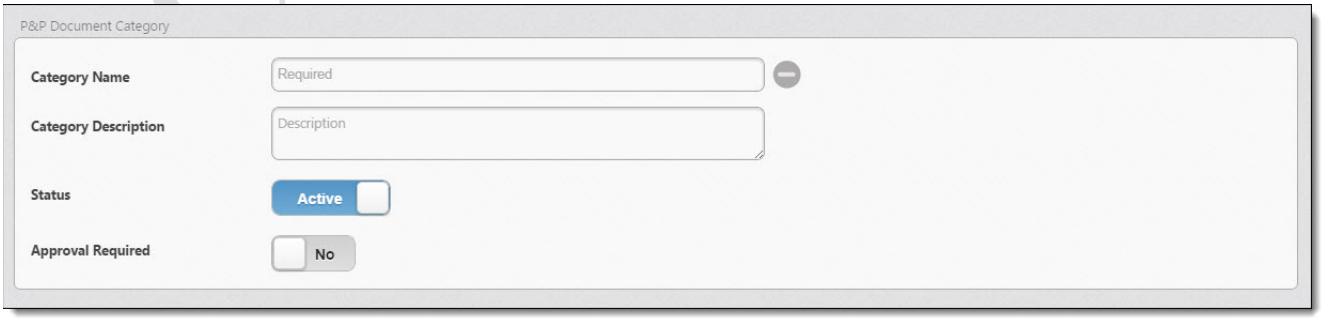


Creating a P&P Document Category

Prior to creating policies and procedures documents, the categories must be created.

1. Select the **Manage P&P Document Categories** link. The Manage P&P Document Categories list will display.
2. To create a P&P document category a user must click on the plus sign. The P&P Documents Details page will display.

When creating a new category a user will be able to update the following fields:



CONFIDENTIAL

- Category Name
  - The category name is required to create a category. The category name must be unique within the client. This field can contain a maximum of 50 alphanumeric characters.
- Category Description
  - This field can contain a maximum of 100 alphanumeric characters and is optional.
- Status
  - This field is a toggle with the option to select a status of Active or Inactive. The default will be set to Active.
  - An inactive category will not be available for a new document. Inactive categories can be reactivated. Any documents belonging to an inactive category are still active and available. A category that has draft documents assigned cannot be deactivated until those documents have been published or deleted.
- Approval Required
  - This field will be a toggle with the options 'Yes' or 'No'. The default will be set to 'No'.
  - If 'Yes' is selected, an 'Assign to' section will be visible displaying Assigned Users. Only one approver can be selected. The selected user will have to approve the document before the publish button is visible, assuming all of the business rules have been satisfied.

3. 'Save' will be enabled once a Category Name is chosen. You can return to the category detail page to make changes at any time. When the Save button is clicked a message will be displayed: 'P&P Document Category successfully saved. Would you like to create a new item or return to the grid?'

Confirmation
P&P Document Category successfully saved. Would you like to create a new category or return to the grid?
Create New Category
Back to Grid

- Clicking *'Create New Category'* will give the user the ability to create a new category.
- Clicking *'Back to Grid'* will direct the user back to the P&P Document Categories page to view the newly created P&P document category.

If a user tries to navigate away from the P&P Document Category Details page without saving, the following message will appear: 'You have unsaved changes. Are you sure you want to leave the page?'

- Clicking *'Ok'* will allow the user to leave the page and discard any changes made.
- Clicking *'Cancel'* will keep the user on the current page.

Important Note: Categories cannot be deleted. They can only be deactivated.

CONFIDENTIAL

Editing a P&P Document Category

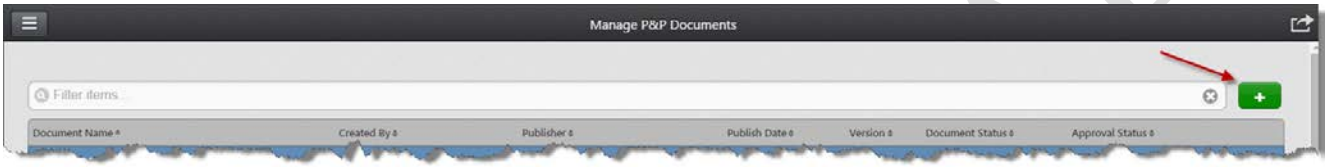
All categories, with the exception of the System Default category, can be edited at any time. Other than the Category Type, all of the category fields are editable. In order to retain your changes you must save before leaving the Category Detail Page.

Managing a P&P Document

In this section, we will discuss how to create and modify documents.

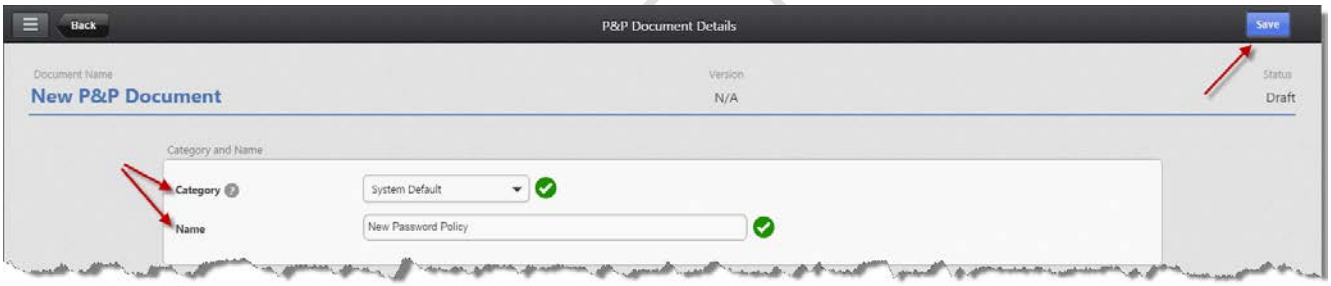
Creating a Document

1. Select the **Manage P&P Documents** link. The Manage P&P Documents list will display.
2. To create a document a user must click on the plus sign.

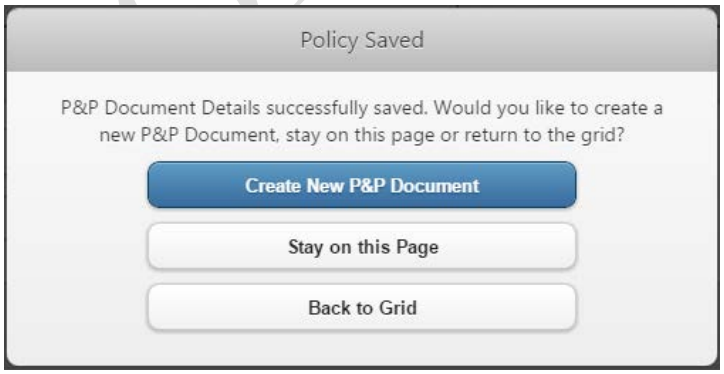


3. Two fields are required to create a document, Category and Name.

   Note: A category must exist before it is available within the Category drop down.

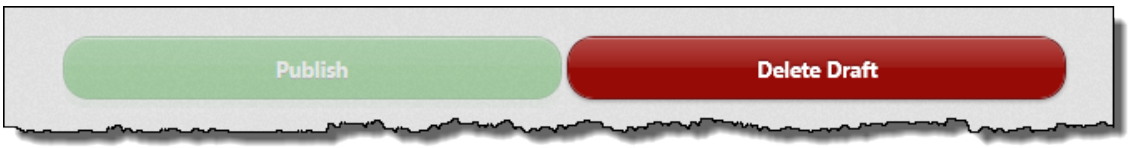


4. The Name must be unique for the category selected. Once the required fields have been completed the 'Save' button will be enabled. Clicking 'Save' will prompt the user with a confirmation of the save and provide three options for the user to choose from: Stay on this Page, New P&P Document, or Back to P&P Grid. These options will only appear for the initial save of a new document.


Policy Saved
P&P Document Details successfully saved. Would you like to create a new P&P Document, stay on this page or return to the grid?
Create New P&P Document
Stay on this Page
Back to Grid

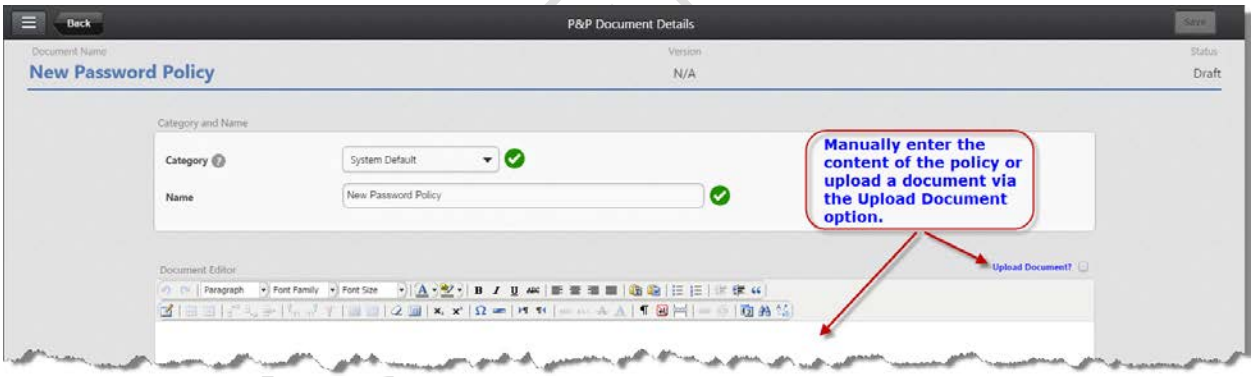
ONLINE

5. After the initial save, buttons will appear at the bottom of the page. If the category requires approval and the user has the Publish function a 'Submit for Approval' button will be shown. If the category does not require approval a 'Publish' button will be shown.



The following fields are available on a document draft:

- Category
  - The category is required to create a document. Inactive categories will not be present in the category drop down. Categories that require approval will be notated with an icon to the right of the category name in the Category drop down. Select the question icon to view the intelligent content for this feature.
- Name
  - The name is required to create a document. The name must be unique for the selected category. This field can contain a maximum of 100 alphanumeric characters.
- Document Editor (three options to create the text associated with the policy).



  - A user can start a document from scratch or the user can copy and paste from a text document. Once the text has been pasted into the document, formatting will be up to the user.
  - The user can upload a document via the **Upload Document** option. Once the document is uploaded, it cannot be edited. If further edits are required, the uploaded document will need to be deleted and an updated one will have to be uploaded.
  - The maximum file size to upload is 10MB.
  - The user will have the ability to view the document content in PDF format by clicking on the PDF Preview button. There must be content within the editor before a document can be published.

Important Notes:

- The file and file name accepts the max of 100 characters and if the attachment document name is more than 50 characters then it will be truncated and displayed.

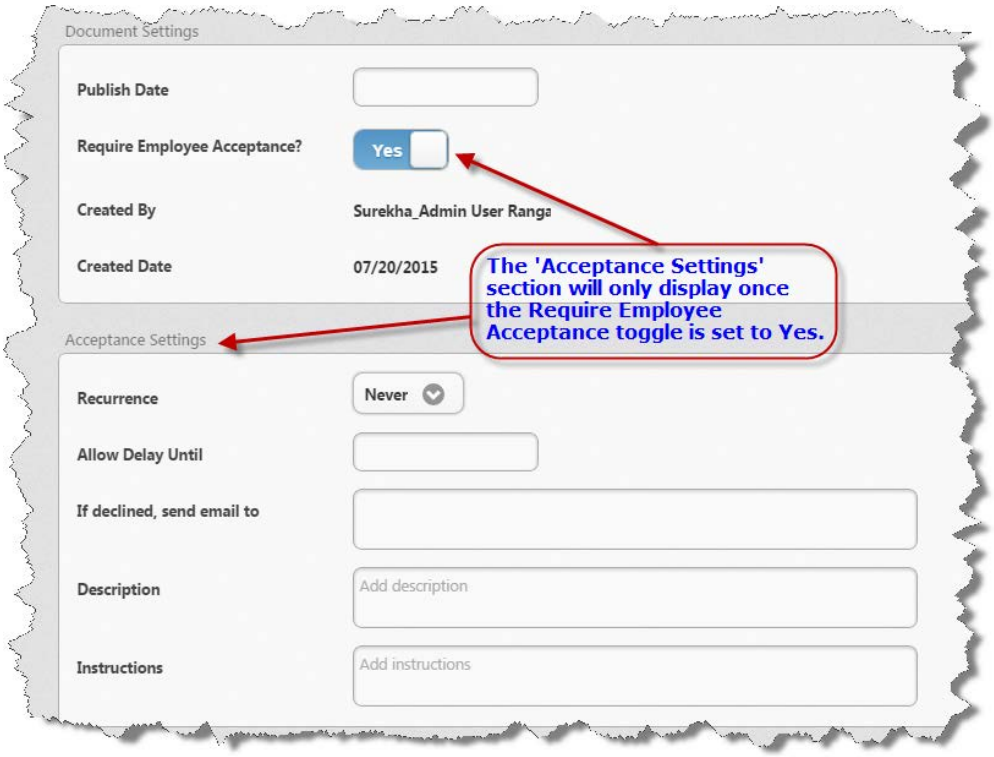
- The file types of doc, pdf, docx, .png, .xls, .xlsx, .gif, .csv, .txt, .bmp, .jpg, and .xml can be uploaded (listed on the upload page).

CONFIDENTIAL

- After uploading and before saving, selecting the Clear button will clear the file, giving the user another opportunity to upload a different file.

- Once the file is uploaded, it cannot be edited. If edits are required, delete the uploaded file and upload the edited version.

If the document requires employees to either accept or decline, the **Require Employee Acceptance** toggle within the Document Settings section must be switched to Yes and the following fields within the Acceptance Settings section will be available on a document draft:



- Recurrence
  - By default, a document will never renew.
  - If a document is set to renew it will renew annually based on the original publish date.
  - A document that renews will have separate reporting for each renewal.
- If declined, send email to
  - A user can enter one or multiple email addresses separated by a semi-colon within this field. Notifications will be sent to these emails if a user declines a document. This field can contain a maximum of 100 alphanumeric characters.
  - The notification message will read as follows:

    Dear Administrator:

    The following user, [First Name Last Name, (UserID)], declined ['Category: Name of the Document'] document on [MM/DD/YYYY].

CONFIDENTIAL

Thanks,

System Support

- Description
  - The description field is for internal use. This field can contain a maximum of 1000 alphanumeric characters.
- Instructions
  - The instructions field will be viewable to the users that are reviewing the document for acceptance. Enter any instructions or comments that you want the user to see when reviewing the document. This field can contain a maximum of 1000 alphanumeric characters.
- Public Document?
  - The Public Document toggle can be set to yes if all active users in the Elite application are required to view the document.
  - If this toggle is set to yes, the **Edit Assigned Users** button will disappear.
  - Public documents are automatically placed in all active users' Document Library.
  - If the document is set to require Employee Acceptance, the Public Document toggle will be disabled.
  - Select the question icon to view the intelligent content for this feature.
- Assigned Users
  - The user can assign one user or all users to a document as long as the Public Document toggle is set to No.
  - A document can be published with no assigned users, but no users will see it until they have been assigned to the document.
  - If a user that was previously assigned is deactivated it will be up to someone with the Manage P&P Document function to remove the user from the Assigned Users List.
- Send Email Notification?
  - This toggle can be set to yes if the creator would like to send an email notification to assigned users.
  - The notification message will read as follows:

    You have a new document to review for acceptance and/or view in your Document Library.

    Document Name: [name of document]
    Created By: [name of document creator]
    Created Date: [date document was created]

    Please log in to WatchDOG Elite to view the document.

- Copy Me?
  - This toggle can be set to yes if the creator would like to also receive an email notification for a document.
  - The Copy Me toggle is only available if the **Send Email Notification** toggle is set to yes.
- Delete Draft Button
  - This will permanently delete the document draft. Only document drafts can be deleted.

The following fields will only be available to a user with the 'Publish P&P Document' function:

- Publish Date
  - The publish date is the day users can view the document for acceptance or in their Document Library if acceptance is not required. The Publish Date must be greater than or equal to the

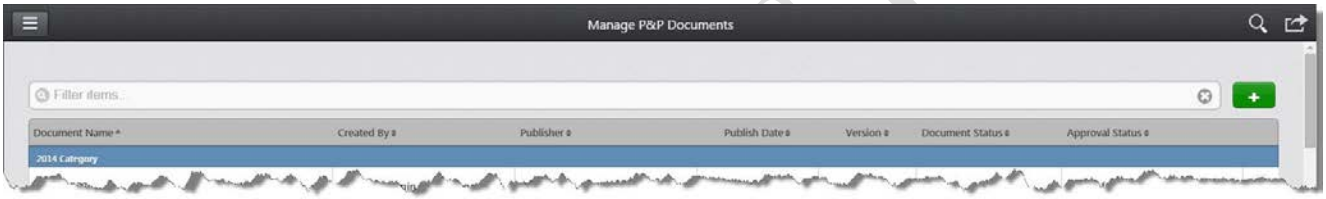
CONFIDENTIAL

current date. The document editor must contain content before a publish date can be set. Once the publish date has been set, any changes made to the title of the document, the document content, or the instructions will clear out the publish date field.

- Allow Delay Until
  - The allow delay until date represents the day the user can no longer delay a document and must Accept or Decline. If this field is left blank the users will not be able to delay the policy once it becomes viewable for acceptance. This field will not be enabled until the publish date is set. The Allow Delay Until date must be greater than or equal to the Publish Date.
- Publish button
  - The publish button will be visible to users who are associated with a role where the Publish P&P Document function is assigned. The Publish button can only be clicked when the Name field has been populated with valid data, document content is present, and the publish date is greater than or equal to the current date. Once published, additional fields will be displayed on the P&P Document Details page: Publisher, Publish Date, and the Archive toggle switch.

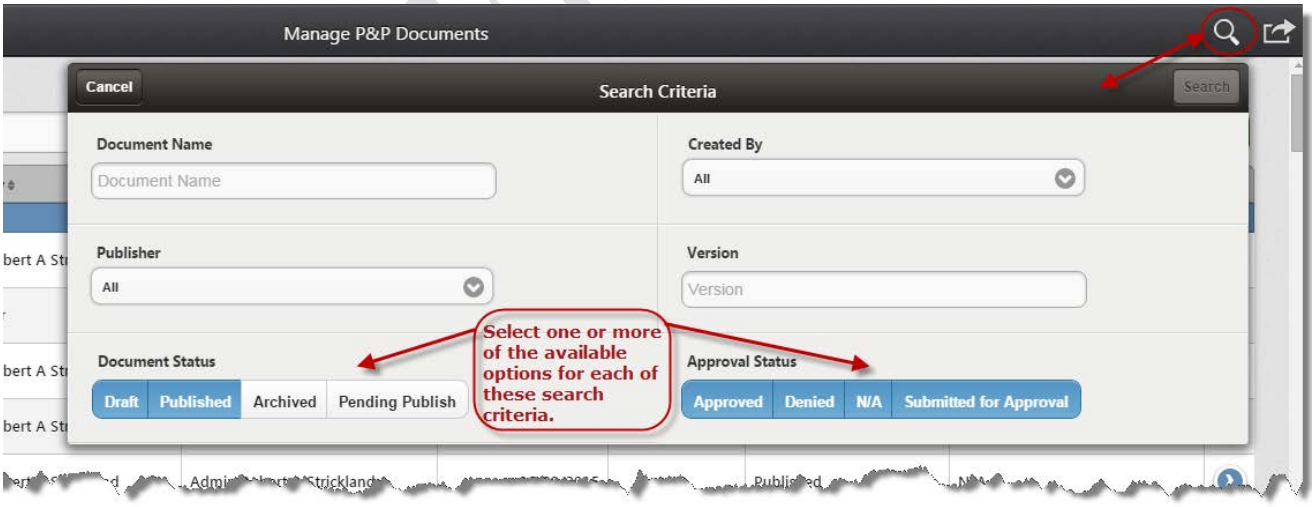
Viewing the Manage P&P Documents Grid

Only the latest version of a document, published or archived, and any drafts will be visible in this grid. The search (filter) bar above the grid can be used to filter the documents in the grid.



Searching the Manage P&P Documents Grid

The logged-in user can perform a search from the Document Library page by selecting the search icon in the top right corner.



Viewing Document Details and Editing a Document

Editable fields are as follows:

Draft Document

- Category
- Name
- Document Editor
- Require Employee Acceptance?
- Recurrence
- If declined, send email to
- Description
- Instructions
- Public Document
- Assigned Users
- Send Email Notification
- Copy Me

Important Note: The fields within the Acceptance Setting section will only be available to edit if the 'Require Employee Acceptance' toggle is set to yes.

Published Document

- Recurrence
- If declined, send email to
- Description
- Archive Toggle
- Assigned Users

Important Note: For a published document, the fields within the Acceptance Settings section listed above and including the 'Allow Delay Until' field will only be available to edit if the document is set to require employee acceptance. Because the 'Require Employee Acceptance' toggle is not editable on a published document, these fields will not be shown if the document did not require employee acceptance at the time it was published.

A user with the Publish P&P Document function can edit these additional fields:

Draft Document

- Publish Date
- Allow Delay Until

Published Document

- Allow Delay Until

After a user has finished editing a document it must be saved.

Note: The only document that can be deleted is a document that has a 'Draft' document status.

CONFIDENTIAL

Publishing a Document that does not Require Approval or Employee Acceptance

A document can be published once the Name, Category, Document Body, and Publish Date fields have been populated. Publishing a document makes it available to users on the document's publish date.

The following actions occur when a document that does not require approval or employee acceptance is published:

On the publish date, users will be able to review the document in their Document Library.

- For publish dates set beyond the current date, documents will be published shortly after 12:00am on the day the document is set to publish.

If the published document is a new version it will cause the previous version to become archived.

Publishing a Document that does not Require Approval but Requires Employee Acceptance

A document with these settings can be published once the Name, Category, Document Body, and Publish Date fields have been populated. Publishing a document makes it available to users on the document's publish date.

The following actions occur when a document that does not require approval but does require employee acceptance is published:

On the publish date, the assigned user(s) will be able to review the document and choose to accept or decline it.

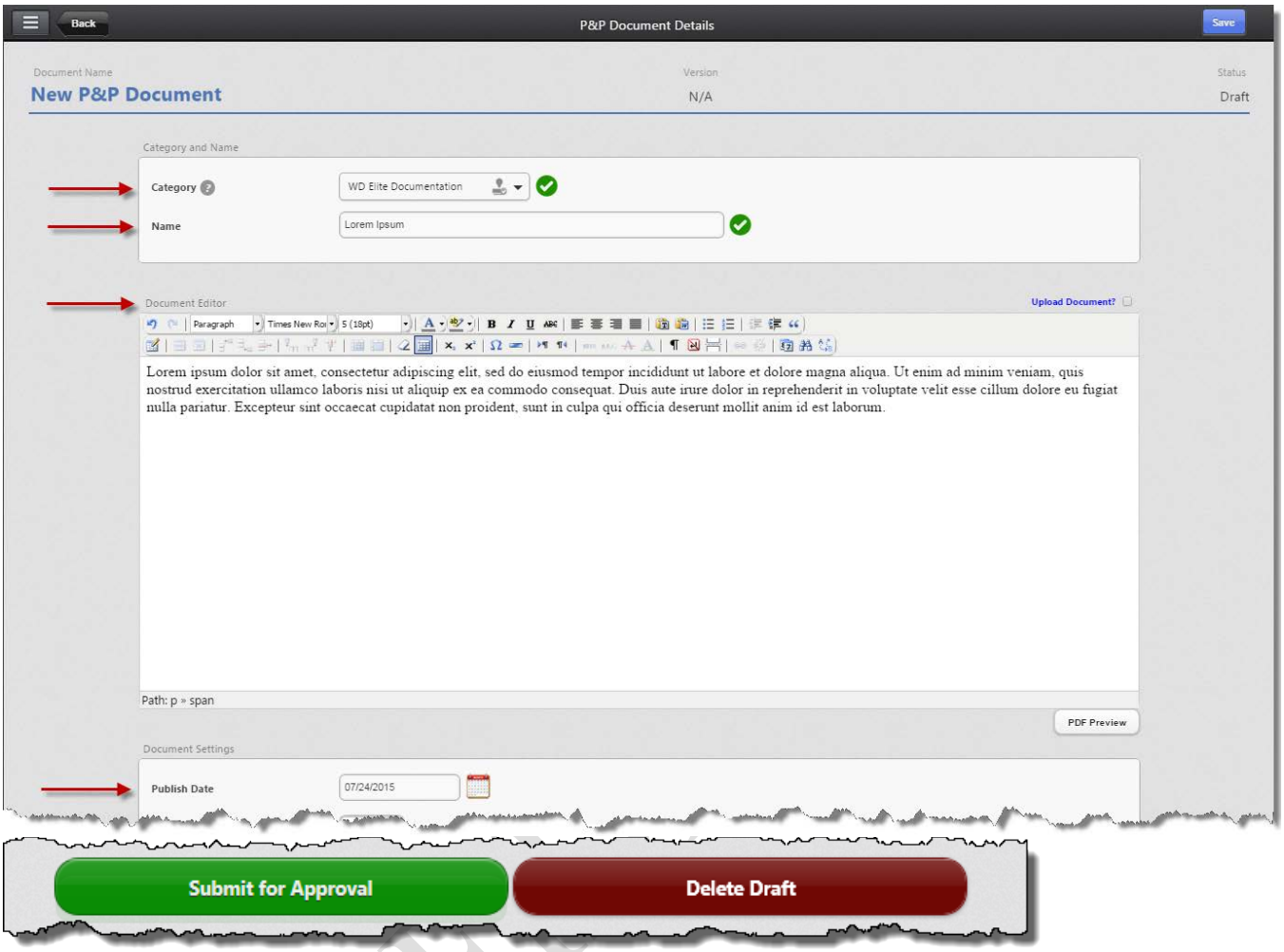
- If an 'Allow Delay Until' date is set, users will be able to delay reviewing a document until that date arrives.
- Once the assigned user(s) selects either to accept, decline or delay the document, the document can then be viewed in the Document Library.
- For publish dates set beyond the current date, documents will be published shortly after 12:00am on the day the document is set to publish.

If the published document is a new version it will cause the previous version to become archived.

Publishing a Document that Requires Approval

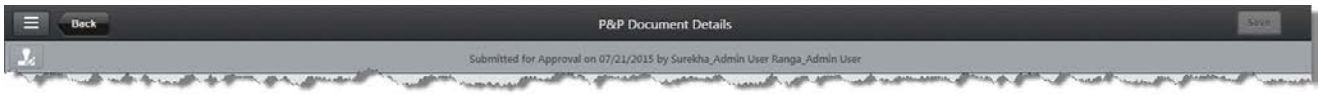
A document can be submitted for approval once the Name, Category, Document Body, and Publish Date fields have been populated.

CONFIDENTIAL

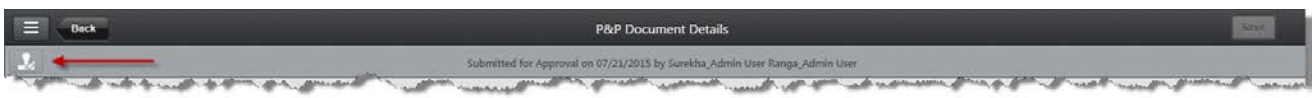

Back
P&P Document Details
Save
Document Name
New P&P Document
Version
N/A
Status
Draft
Category and Name
Category
WD Elite Documentation
Name
Lorem Ipsum
Document Editor
Upload Document?
Paragraph
Times New Roi
5 (18pt)
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.
Path: p » span
PDF Preview
Document Settings
Publish Date
07/24/2015
Submit for Approval
Delete Draft

The following events occur when a document is submitted for approval:

- An email is sent to the approver.
  - The email includes a hyperlink that will take the approver to the application login page.
- The document approval status changes from 'N/A' to 'Submitted for Approval'.
- All fields are locked down for any user except the document creator.
  - The document creator is able to make changes, but the approver will only be notified of the changes if the creator selects the 'Submit Changes for Approval' button.
- A gray bar appears on the document detail page showing the name of the user that submitted the document for approval and when the document was submitted.



- On the left side of the gray bar is a button that slides open the Approval and Comments section.



- The comments will stay with the document for the life of the document.
- The actions Approve, Deny, Reset, and Submit changes will create an entry with a timestamp in the comments.
- The assigned approver will have the option to approve or deny the document from this section.

➢ The buttons 'Submit Changes for Approval', 'Reset', and 'Delete' are available

- 'Submit Changes for Approval' is used to notify the assigned approver that changes have been made to the document. This button will reset any Approval Status back to 'Submitted for Approval'.
- 'Reset' is used when the assigned approver for the category has been changed. The new assigned approver will receive an email notifying them that a document has been submitted to them for approval.
- 'Delete' will permanently erase the draft document, including any comments that are attached to it.

During the approval process, the approver will need to review the submitted document. The document can be found on the Manage P&P Documents page and will be located under the category in which the document was created. It will have a status of 'Ready for Approval'.

The approver can choose to either approve or deny the document from the approval slide over.

If a document is denied:

- An email is sent to the submitter letting them know that their document has been denied.
- The Document Approval Status is set to 'Denied'.

If a document is approved:

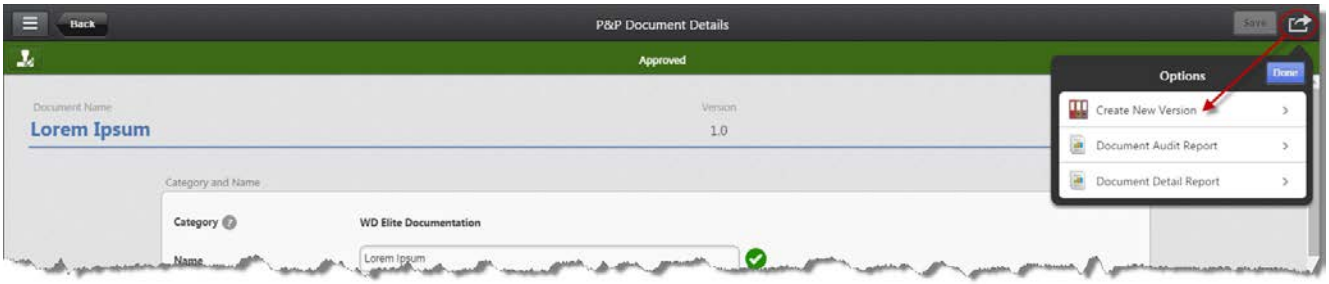
- An email is sent to the submitter letting them know that their document has been approved.
- The Document Approval Status is set to 'Approved'.

CONFIDENTIAL

- The 'Publish' button will replace the 'Submit Changes for Approval' button and is available for use only by the submitter.

Creating a New Version of a Document

A user is able to create a new version of a document from the Document Details Page of a published document. The 'Create New Version' link is found under the 'Options' button located in the top right hand corner of the screen.



Creating a new version of a document will carry over all fields except the 'Publish Date' and 'Allow Delay Until' fields. The new version is created as a draft which means that all fields are editable.

There can only be one draft for any given document chain. If the user has created a new version draft, the 'Create New Version' option on the published documents detail page will now read 'View Draft'. Clicking 'View Draft' will take you to the detail of that version draft.

Once you publish a draft of a previously published document, that draft will have the highest version number for the chain. The previously published version will be automatically archived. The archived version will be viewable within the Version History grid on the detail page for that document chain.

Each Version is tracked separately for auditing and reporting purposes.

Archiving a Document

A user with the Manage P&P Documents function can archive a document manually by viewing the detail of a document and switching the archive toggle to 'Yes' and clicking 'Save'.

If archived, the document will not be editable or visible to any end users.' An archived document cannot be un-archived. All auditing and reporting information for archived documents is retained.

Published documents that are replaced by a new version of that document chain will be automatically archived.

Viewing a Document's Version History

Users can view the history of a document by viewing the Document Details Page. If the document chain has multiple versions of a document the user will be able to view the Version History at the bottom of the P&P Document Details page. Selecting one of the historical documents will open it in a read-only format.

CONFIDENTIAL

P&P Document Review for Users

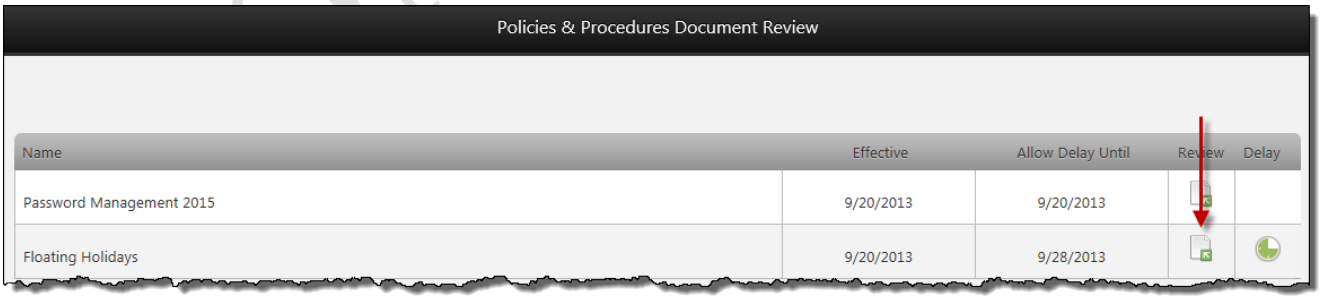
In this section we will review how individual users will login to accept, deny or delay documents to which they are assigned.

Viewing Documents for Acceptance

These documents are presented upon the user login to the WatchDOG Elite application. The P&P Document Review page will overlay the Getting Started page. They will not be able to navigate away from the P&P Document Review page until all documents have been reviewed.

From the main grid of the P&P Document Review page users can delay any document that has an 'Allow Delay Until' date that is set in the future. If all documents can be delayed, there will be a Delay All button at the bottom of the grid. Once a single document cannot be delayed, the Delay All button will no longer be available.

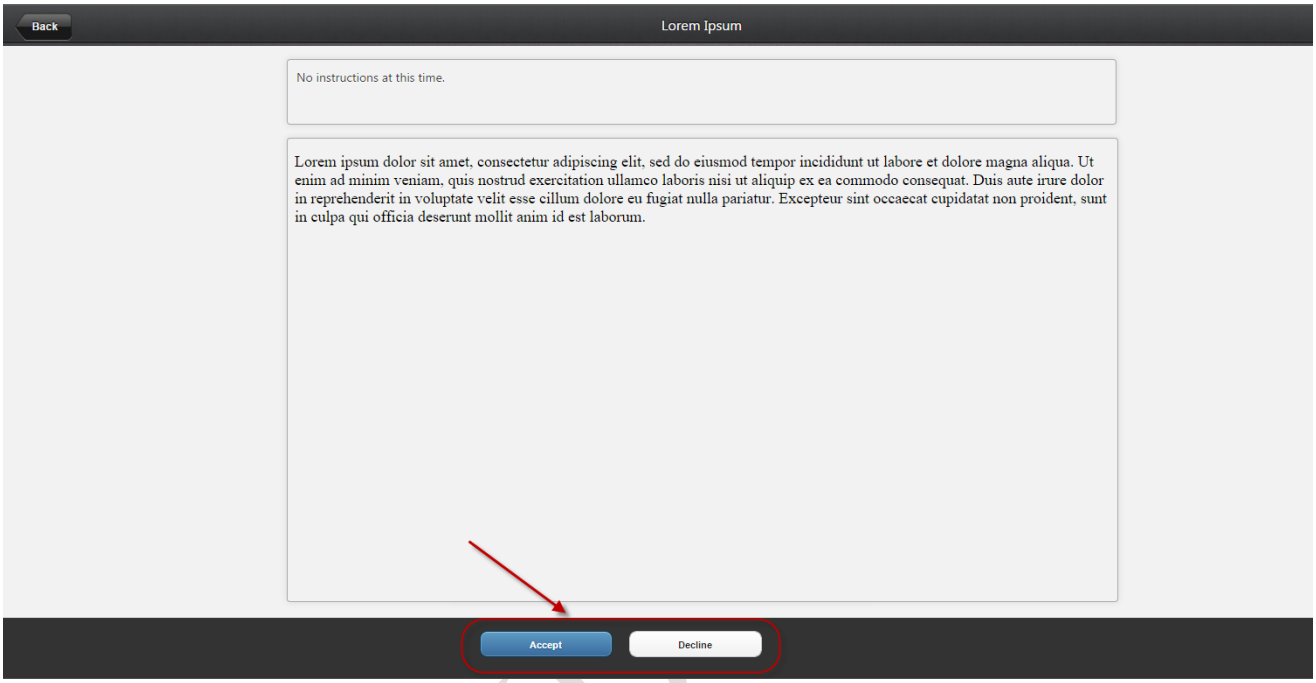
To review a document, a user will need to select the review icon for the document they wish to review.



Important Note: If the document policy was uploaded, instead of written in the text editor, the end user will need to perform another step after selecting the review icon. After selecting the icon, another page will display a View Document button. Select the button to review the document. Close after reviewing and then Accept or Decline the policy.

CONFIDENTIAL

The document will be presented with the instructions and the read only text of the document they are reviewing. Once the document has been reviewed, the user will have the ability to Accept, Decline, or Delay (if available) using the buttons at the bottom of the page. Users are able to print the document from the document review page.


Back
Lorem Ipsum
No instructions at this time.
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.
Accept
Decline

Once all of the documents assigned to the user have been accepted, declined, or delayed the user will be able to enter the application as usual.

CONFID

P&P Reporting

There are several reports associated to the P&P module. The reports to which you have access will be available.

Document Summary Report

The Document Summary Report can be found in the Options menu of the Manage P&P Documents Page. This report is a snapshot of the current state of all documents that have been created. This report can be filtered to narrow it down to as few as one document.

User Document Action Report

The Document Action Report can be found in the Options menu of the Manage P&P Documents Page. This report is a snapshot of all user decisions for all documents. This will display if a user has accepted, declined, delayed, or not yet reviewed a document they have been assigned to.

Document Audit Report

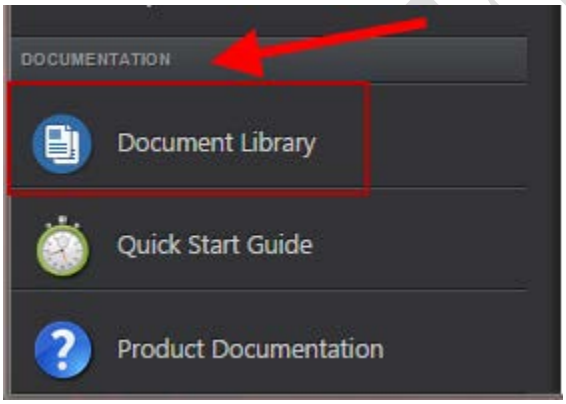
The Document Audit Report can be found in the Options menu of the P&P Document Details Page. This report provides an audit trail of all changes made to a published document. This report will only display information for the document it is opened from.

Document Detail Report

The Document Detail Report can be found in the Options menu of the P&P Document Details Page. This report is a snapshot of the actions users have taken on the document it is opened from.

Document Library

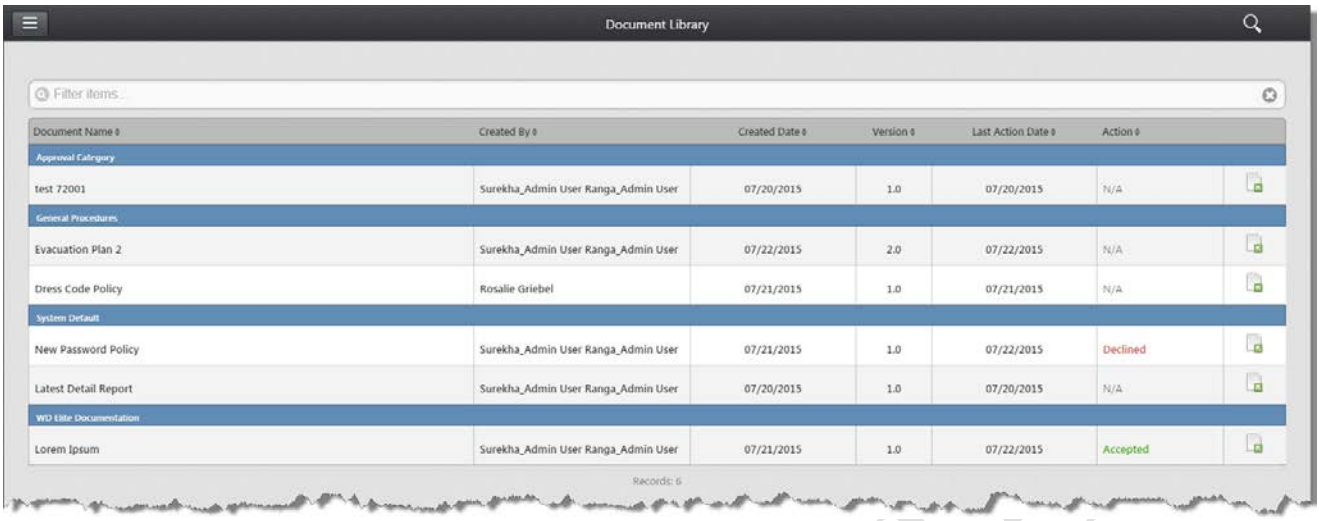
The Document Library allows the current logged in user to view all documents assigned to them. The Document Library link is located under the Documentation section in the side Navigation bar and will be visible to all active WatchDOG Elite users.



Important Note: Currently, documents must be created and assigned to users within the Policies &Procedures area of the WatchDOG Elite application in order to be viewed in the Document Library.

Documents that have been Accepted, Delayed, or Declined can be viewed in the Document Library. In addition to these, documents that did not require employee acceptance but were made public or assigned to the logged in user can be viewed here as well.

CONFIDENTIAL



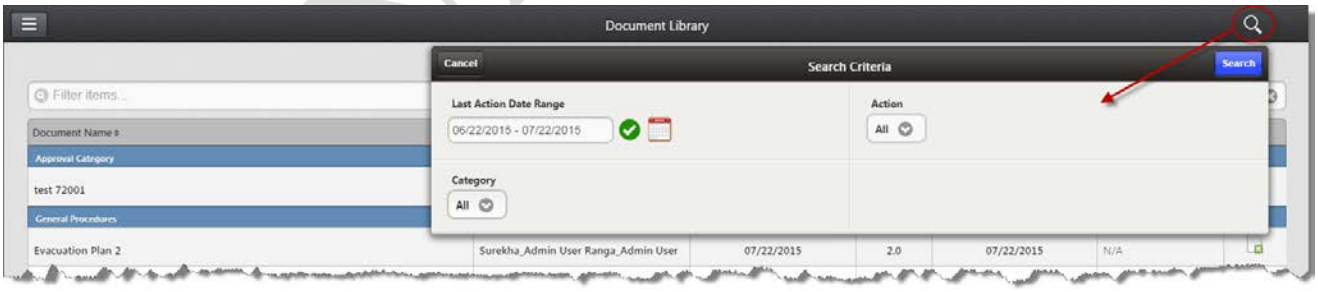
The Document Library will display the following data for each item in the grid:

- Document Name
- Created By
- Created Date
- Version
- Last Action Date
- Action

The user can select the icon to display a read-only view of the document.

Document Library Search

The logged-in user can perform a search from the Document Library page by selecting the search icon in the top right corner.



Select the **Last Action Date Range** via the calendar control, and/or the **Action** via the drop down and click the Search button to retrieve results.

This completes the Policies and Procedures section.

CONFIDENTIAL

SmartRisk IQ Overview

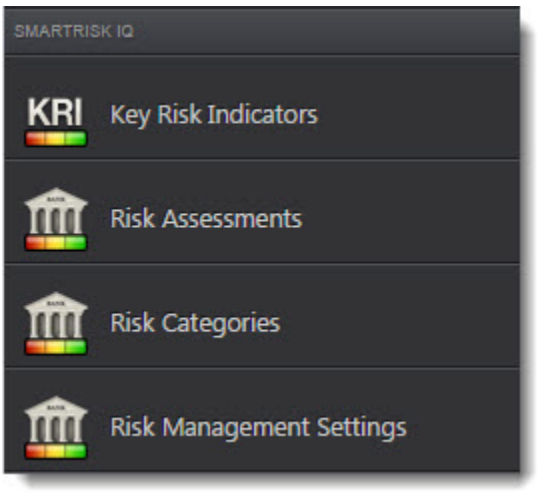
This section of the Elite Quick Start guide details the steps to create and manage Risk Assessments, as well as view the eight OCC Risk Categories, set risk tolerances via the Settings, and complete Key Risk Indicator metrics.

Important Note: This guide is written with the assumption that all roles and users have been defined and created within the application. Please see Chapter 11 in the full user manual, which can be accessed via the Product Documentation link in the Navigation toolbar, for a more detailed explanation of all functions and reports as well as the functions required to access the features and functionality.

Navigation:

Most of the navigation within the application is driven through the left side Navigation toolbar.

Only those links which the user has access to via security functions will be available in the Navigation toolbar. For SmartRisk IQ, the section will be displayed as:



Risk Management Settings

Let's start with your Risk Management Settings. The WatchDOG Elite Risk Management system is built on the OCC Risk Management regulatory guidelines and framework. There are eight (8) risk categories defined by the OCC that should be monitored and assessed for compliance.

- Compliance Risk
- Credit Risk
- Interest Rate Risk
- Liquidity Risk
- Operational Risk
- Price Risk
- Reputational Risk
- Strategic Risk

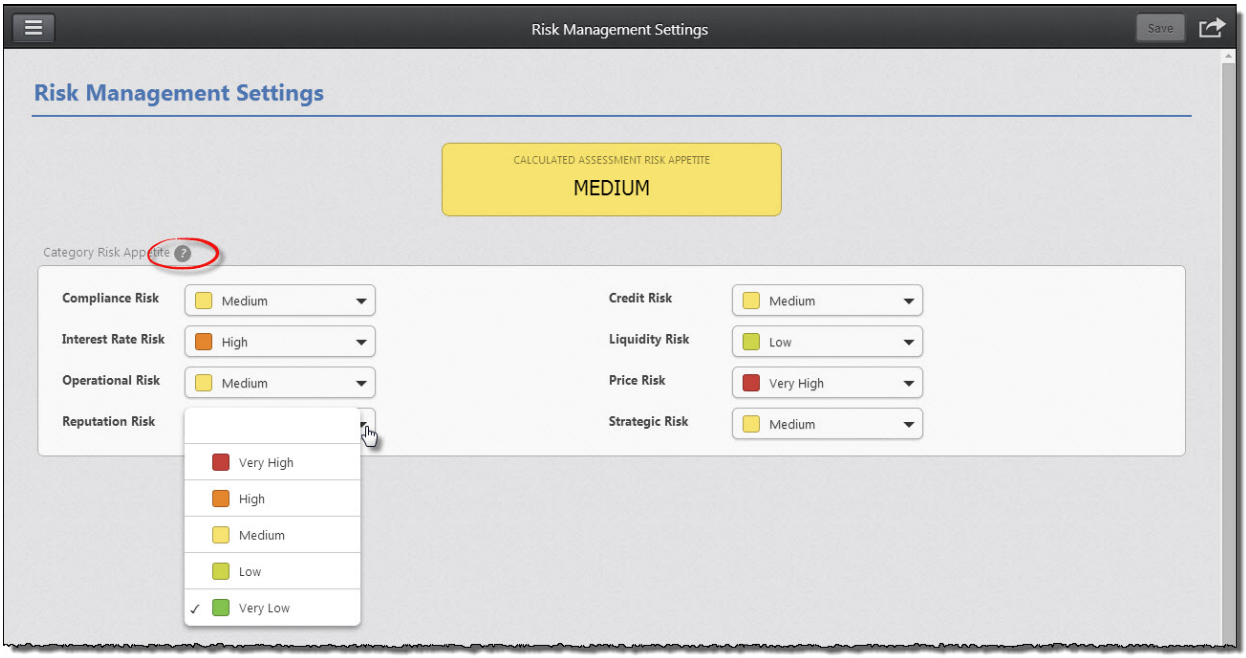
The Risk Management Settings page allows you to set your tolerance or risk appetite for each of the eight Risk Categories – to determine the amount of risk you are willing to accept in each area.

The tolerances you set here in the Settings will be compared to your actual risk levels on each Risk Assessment you complete.

CONFIDENTIAL

Category Risk Appetite

To set the risk appetite for each Risk Category, select the **Risk Management Settings** option in the left side bar menu.



A screen will appear listing all eight Risk Categories with drop down menus beside each one.

To set your Risk Appetite for each category, select it from the menu beside the desired category name.

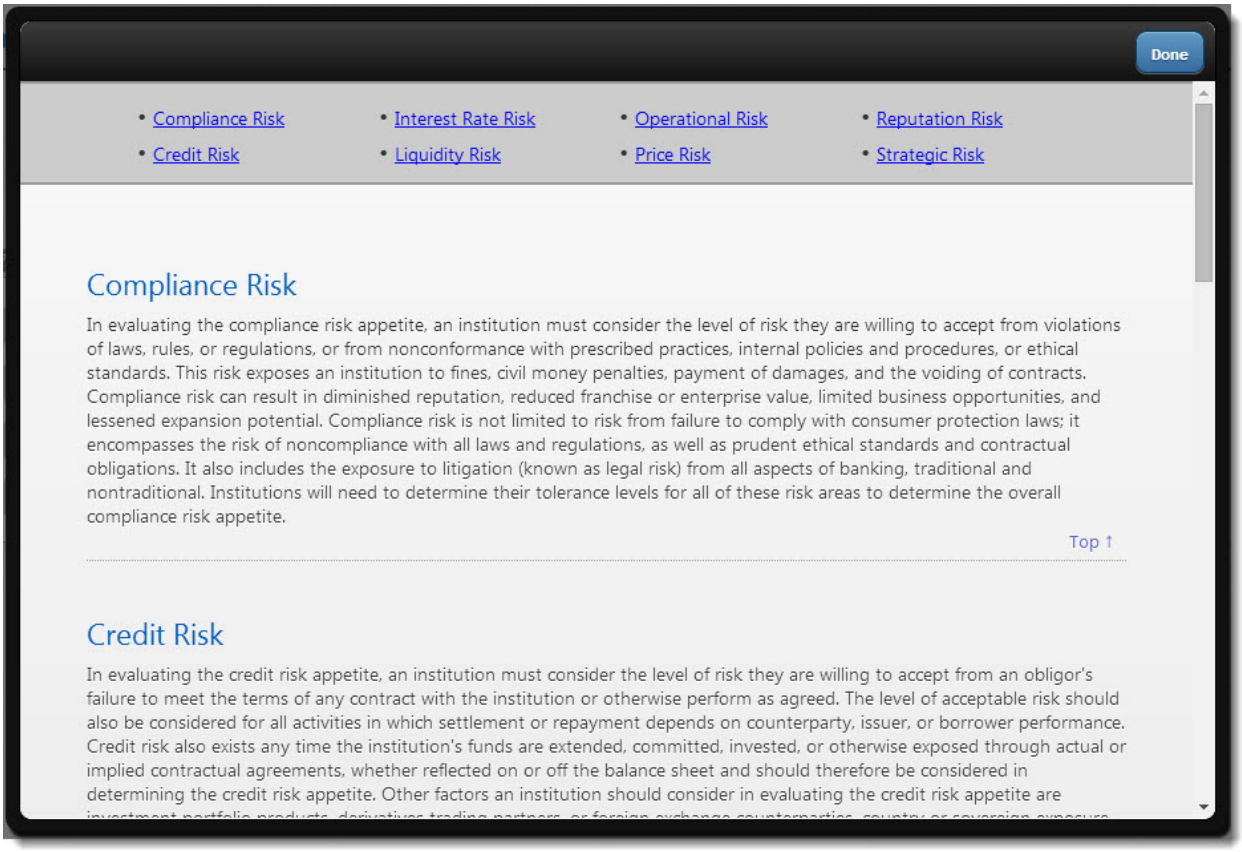
When you have set all your tolerance levels, select **Save** in the top right corner of the screen to save your settings.

Notice that an overall Calculated Assessment Risk Appetite appears at the top of the screen. This is a system calculated value that averages the appetite levels selected for all categories and gives you an overall Risk Appetite for your assessments.

If you determine that your overall Assessment Risk Appetite is too high or low, adjust the individual risk levels on your Risk Categories.

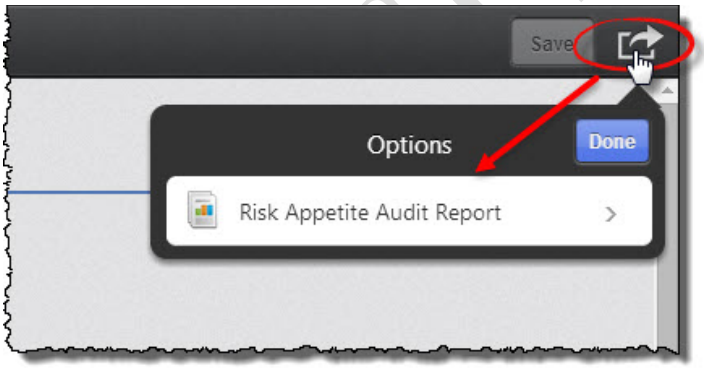
Important Note: Intelligent Content is available by clicking the question mark icon beside the Category Risk Appetite field label. This will display a pop-up that provides guidance about setting your risk appetite by category.

CONFIDE

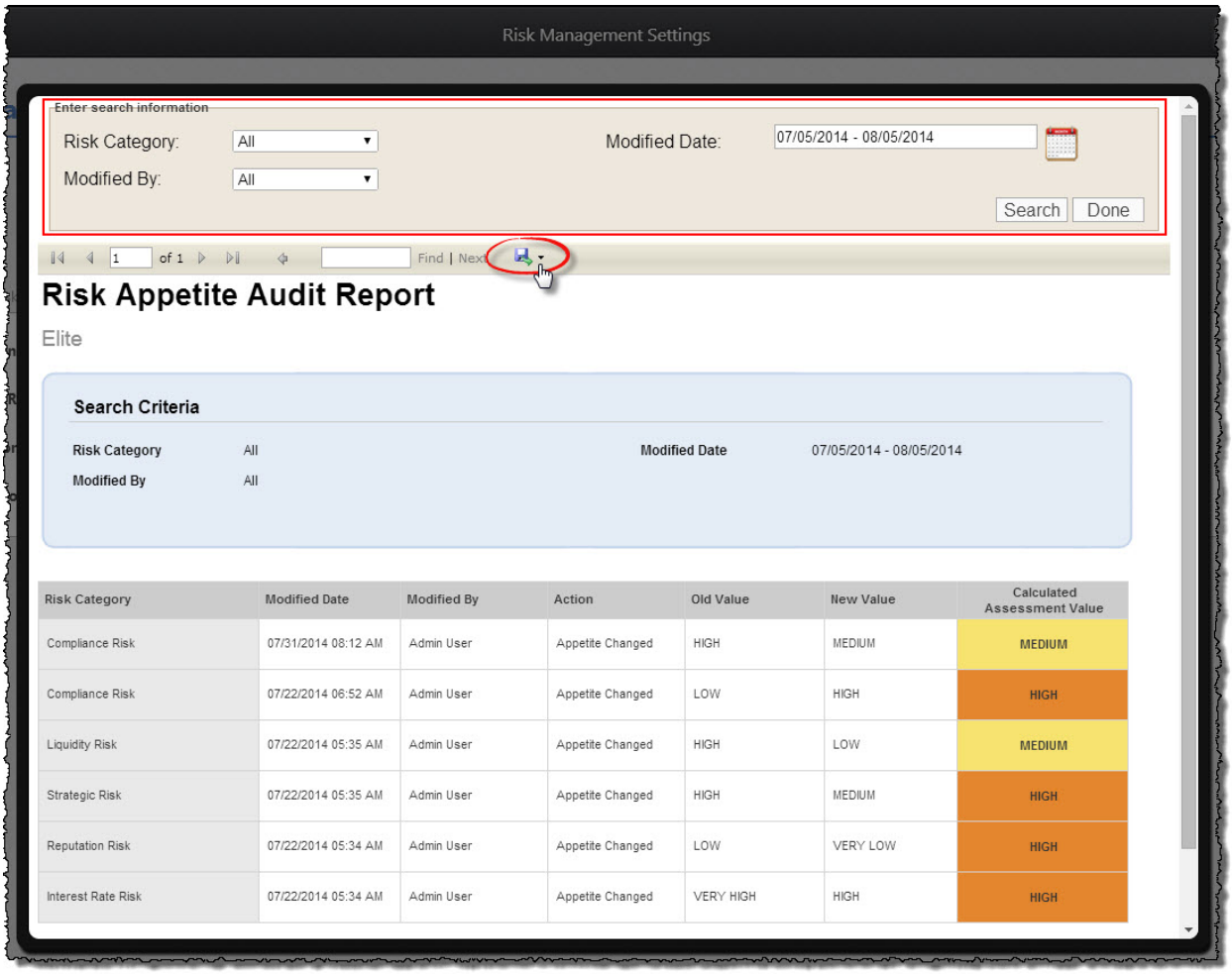

Done
• Compliance Risk
• Credit Risk
• Interest Rate Risk
• Liquidity Risk
• Operational Risk
• Price Risk
• Reputation Risk
• Strategic Risk
Compliance Risk
In evaluating the compliance risk appetite, an institution must consider the level of risk they are willing to accept from violations of laws, rules, or regulations, or from nonconformance with prescribed practices, internal policies and procedures, or ethical standards. This risk exposes an institution to fines, civil money penalties, payment of damages, and the voiding of contracts. Compliance risk can result in diminished reputation, reduced franchise or enterprise value, limited business opportunities, and lessened expansion potential. Compliance risk is not limited to risk from failure to comply with consumer protection laws; it encompasses the risk of noncompliance with all laws and regulations, as well as prudent ethical standards and contractual obligations. It also includes the exposure to litigation (known as legal risk) from all aspects of banking, traditional and nontraditional. Institutions will need to determine their tolerance levels for all of these risk areas to determine the overall compliance risk appetite.
Top ↑
Credit Risk
In evaluating the credit risk appetite, an institution must consider the level of risk they are willing to accept from an obligor's failure to meet the terms of any contract with the institution or otherwise perform as agreed. The level of acceptable risk should also be considered for all activities in which settlement or repayment depends on counterparty, issuer, or borrower performance. Credit risk also exists any time the institution's funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether reflected on or off the balance sheet and should therefore be considered in determining the credit risk appetite. Other factors an institution should consider in evaluating the credit risk appetite are

Risk Appetite Audit Report

Select the Options menu icon in the top right corner of the Risk Management Settings screen to access a Risk Appetite Audit Report.



This report provides a detailed list of all the changes that have been made to your Category Risk Appetite settings over time.



Risk Category	Modified Date	Modified By	Action	Old Value	New Value	Calculated Assessment Value
Compliance Risk	07/31/2014 08:12 AM	Admin User	Appetite Changed	HIGH	MEDIUM	MEDIUM
Compliance Risk	07/22/2014 06:52 AM	Admin User	Appetite Changed	LOW	HIGH	HIGH
Liquidity Risk	07/22/2014 05:35 AM	Admin User	Appetite Changed	HIGH	LOW	MEDIUM
Strategic Risk	07/22/2014 05:35 AM	Admin User	Appetite Changed	HIGH	MEDIUM	HIGH
Reputation Risk	07/22/2014 05:34 AM	Admin User	Appetite Changed	LOW	VERY LOW	HIGH
Interest Rate Risk	07/22/2014 05:34 AM	Admin User	Appetite Changed	VERY HIGH	HIGH	HIGH

The report includes the Risk Category, the date on which that category's appetite was changed, who made the change, what action was taken, what the previous value was, what the new value is, and how that affected the Calculated Assessment Value.

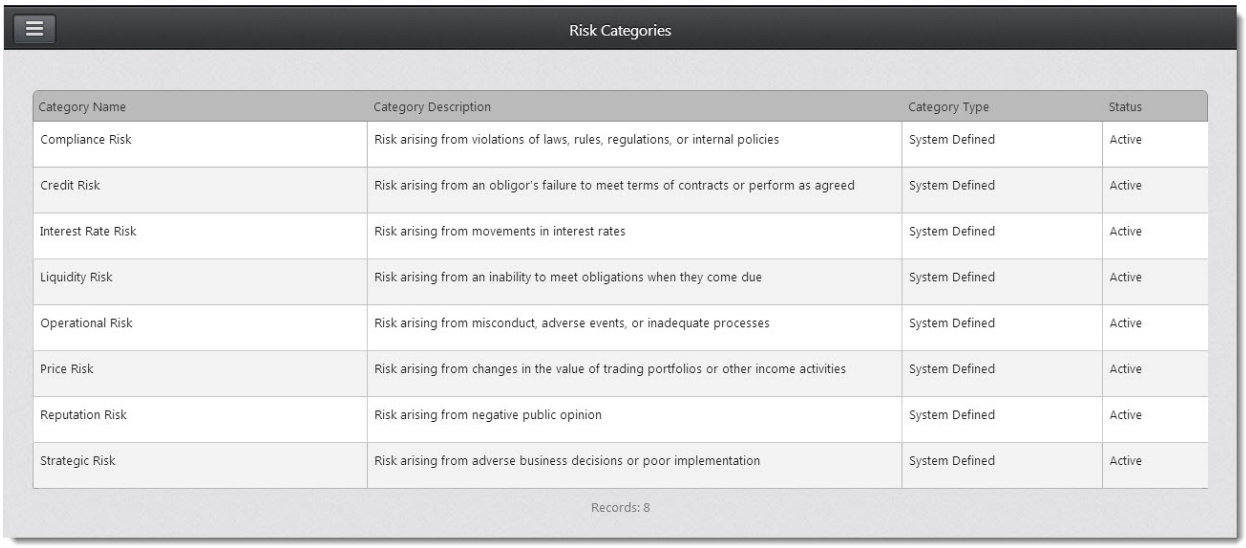
You can search and filter the report using the criteria provided.

This report can be exported to Excel, PDF, or Word.

Risk Categories

Selecting the **Risk Categories** menu option under SmartRisk IQ will display a list of the eight Risk Categories from the OCC that are standard to the Elite Risk Management application.

CONFIDENTIAL



Category Name	Category Description	Category Type	Status
Compliance Risk	Risk arising from violations of laws, rules, regulations, or internal policies	System Defined	Active
Credit Risk	Risk arising from an obligor's failure to meet terms of contracts or perform as agreed	System Defined	Active
Interest Rate Risk	Risk arising from movements in interest rates	System Defined	Active
Liquidity Risk	Risk arising from an inability to meet obligations when they come due	System Defined	Active
Operational Risk	Risk arising from misconduct, adverse events, or inadequate processes	System Defined	Active
Price Risk	Risk arising from changes in the value of trading portfolios or other income activities	System Defined	Active
Reputation Risk	Risk arising from negative public opinion	System Defined	Active
Strategic Risk	Risk arising from adverse business decisions or poor implementation	System Defined	Active

Records: 8

These categories are currently read-only and active by default. In a future release of SmartRisk IQ, users will have the ability to deactivate system categories and add their own custom categories.

Key Risk Indicators

In the context of SmartRisk IQ, the Key Risk Indicators are intended to assist the Risk team in answering the Risk Assessment questionnaire more quantitatively or objectively, using key metrics and factual data about the institution's performance at the time of the assessment to support accurate responses to the assessment questions.

A little less than half of the current Key Risk Indicator library in Elite are automatically being populated using information specific to your institution from the Uniform Bank Performance Report (UBPR) provided by the Federal Financial Institutions Examination Council (FFIEC). The rest of the indicators must be completed manually by your institution.

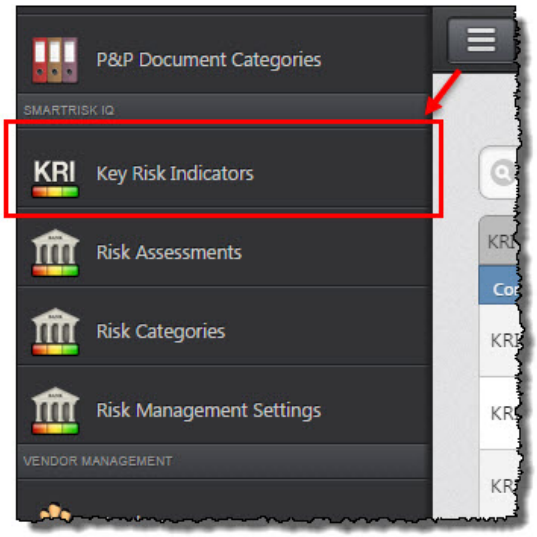
Key Risk Indicators that have a value, either pulled from the UBPR or entered manually by a user of the platform, will be displayed beneath their corresponding assessment questions on Risk Assessments as long as you've enabled them to show on the assessment.

The Key Risk Indicator library currently contains indicators that have been defined by CSI Regulatory Compliance. You are not currently able to add custom indicators or change the indicator descriptions for these system indicators. The ability to create user-defined indicators will be available in a future release.

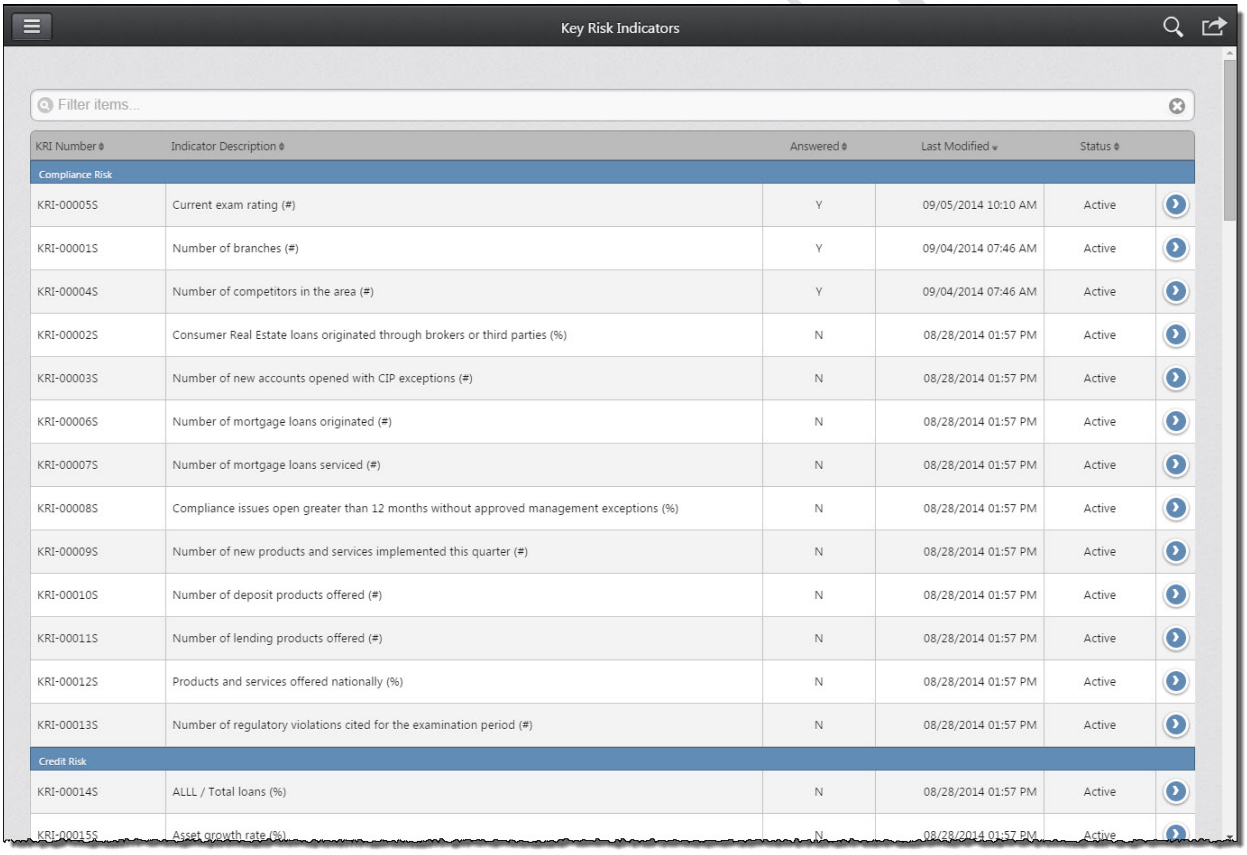
Manage Key Risk Indicators

To view and manage your library of Key Risk Indicators, select the **Key Risk Indicators** menu option found under the SmartRisk IQ area of the left side menu.

CONFIDENTIAL

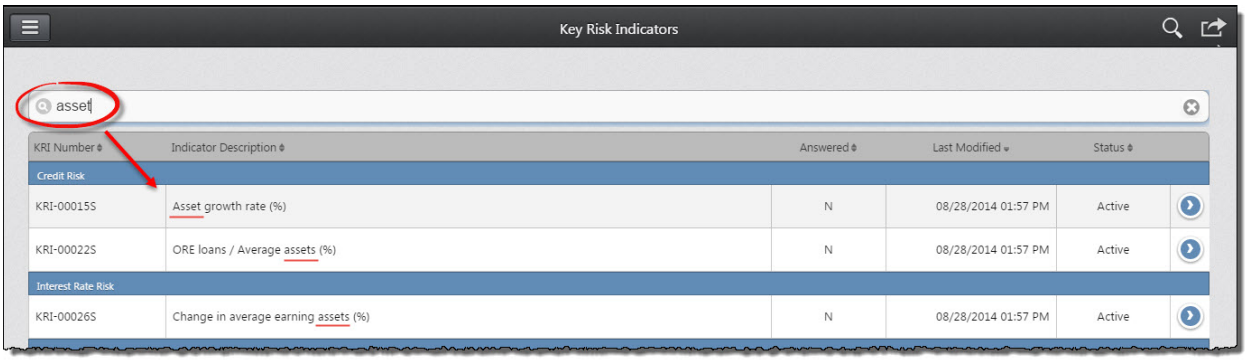


A grid listing the library of indicators will display.

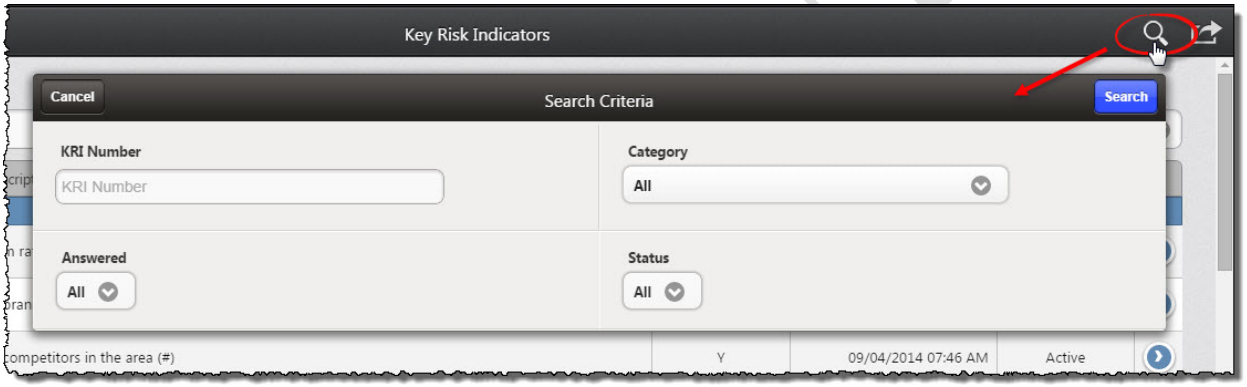

Key Risk Indicators
Filter items...
KRI Number
Indicator Description
Answered
Last Modified
Status
Compliance Risk
KRI-00005S Current exam rating (#) Y 09/05/2014 10:10 AM Active
KRI-00001S Number of branches (#) Y 09/04/2014 07:46 AM Active
KRI-00004S Number of competitors in the area (#) Y 09/04/2014 07:46 AM Active
KRI-00002S Consumer Real Estate loans originated through brokers or third parties (%) N 08/28/2014 01:57 PM Active
KRI-00003S Number of new accounts opened with CIP exceptions (#) N 08/28/2014 01:57 PM Active
KRI-00006S Number of mortgage loans originated (#) N 08/28/2014 01:57 PM Active
KRI-00007S Number of mortgage loans serviced (#) N 08/28/2014 01:57 PM Active
KRI-00008S Compliance issues open greater than 12 months without approved management exceptions (%) N 08/28/2014 01:57 PM Active
KRI-00009S Number of new products and services implemented this quarter (#) N 08/28/2014 01:57 PM Active
KRI-00010S Number of deposit products offered (#) N 08/28/2014 01:57 PM Active
KRI-00011S Number of lending products offered (#) N 08/28/2014 01:57 PM Active
KRI-00012S Products and services offered nationally (%) N 08/28/2014 01:57 PM Active
KRI-00013S Number of regulatory violations cited for the examination period (#) N 08/28/2014 01:57 PM Active
Credit Risk
KRI-00014S ALLL / Total loans (%) N 08/28/2014 01:57 PM Active
KRI-00015S Asset growth rate (%) N 08/28/2014 01:57 PM Active

The grid displays a system-generated KRI Number, available simply for reference, for each indicator. The Indicator Description or name is provided in the grid, along with an Answered column to specify which indicators have a value already provided and which need to be completed. Finally, the grid includes the Last Modified date and the status that shows whether the indicator is Active or Inactive.

The indicators are grouped by Risk Category to make it easier to find similar or related indicators. You can also find indicators more easily by using the Filter items search above the grid. Simply start typing a key word or phrase and the list will automatically filter for those terms.



Additionally, you can search for indicators using the **Search** option. Select the magnifying glass icon in the top right corner of the Key Risk Indicators screen to open the search window.



Enter a KRI reference number to search for a specific indicator if you know its number.

Select a Category to search for the indicators grouped into a specific Risk Category.

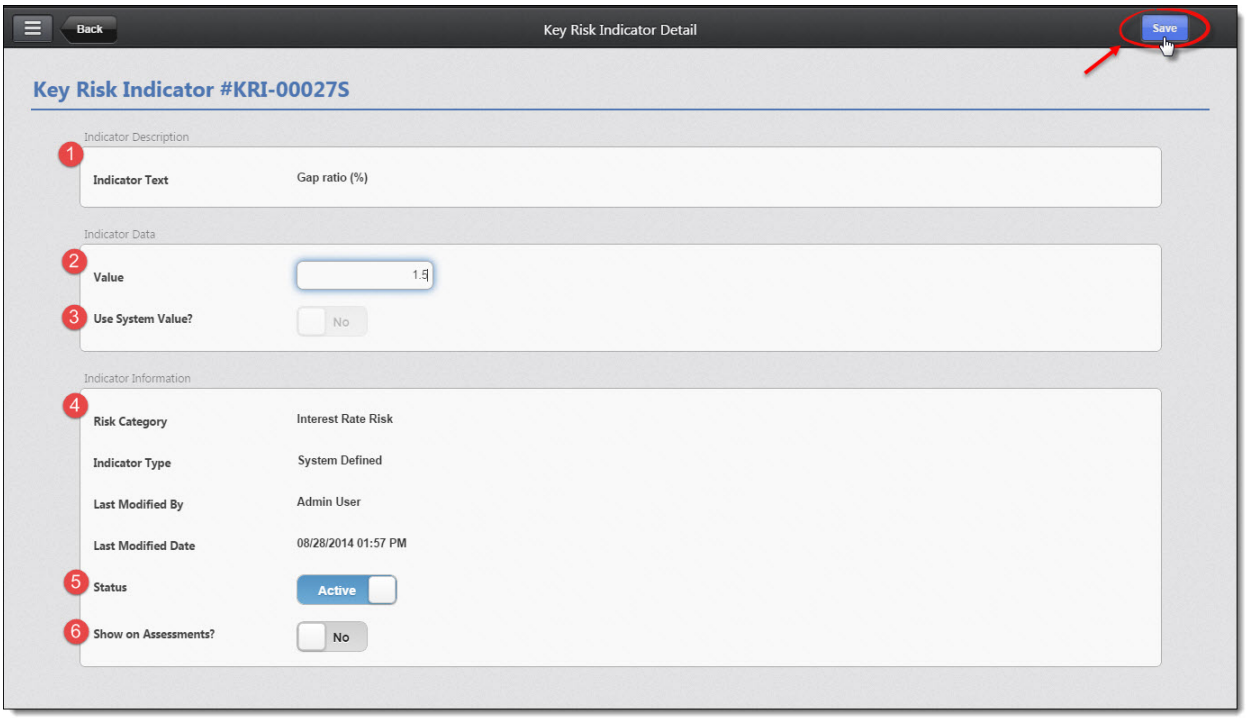
Select Yes or No to search for the indicators that do or do not have data values already assigned to them.

Select Active or Inactive to search for the indicators that have been set to an active or inactive status.

Key Risk Indicator Details

To access the details of a specific indicator, select the arrow icon on the right hand side of the desired row or click anywhere in the row.

The Key Risk Indicator Detail page will display.

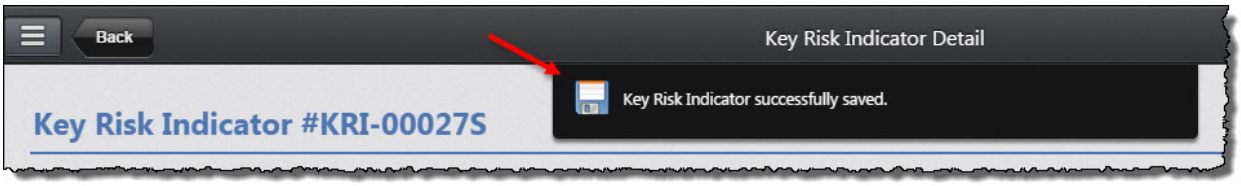


The available fields on the Key Risk Indicator Detail screen include:

1. Indicator Text Description – This field displays read-only text that describes the indicator. System Defined KRI descriptions cannot be edited.
2. Value – This field represents the actual value of the indicator for your institution for the current period. This field is audited, so any changes to the value over time are saved and stored for future reference; however, the value displayed is always the most recently entered and saved value.
   ** Note that the Indicator Text Description contains a symbol representing the type of value the indicator should be provided in, i.e. a percent (%), a number (#), or a dollar amount ($).*
3. Use System Value? – This field allows you to toggle between using the value that is pulled from the UBPR versus overriding the UBPR value and entering your own. This field will only be editable for indicators that can and are being populated from the UBPR.
4. Indicator Type – This read-only information provides general system data about the indicator, including the Risk Category it is assigned to, the Indicator Type (defined by the System or customized by a user), the user who Last Modified the indicator, and the Last Modified Date.
5. Status – Use the status field to deactivate an indicator you do not want to use anywhere in the system, including on assessments. Inactive indicators will continue to display on the Key Risk Indicators list unless you remove them using the Search feature, but they will not display on Risk Assessments.
6. Show on Assessments? – This field controls whether the Indicator Description and Value will be displayed on relevant assessment questions. Make sure you change this to Yes before saving the value if you want the indicator to show on assessments.

CONFIDE

Once you have updated the Key Risk Indicator Detail, be sure to **Save** your changes. A confirmation message will display when the indicator is saved successfully.

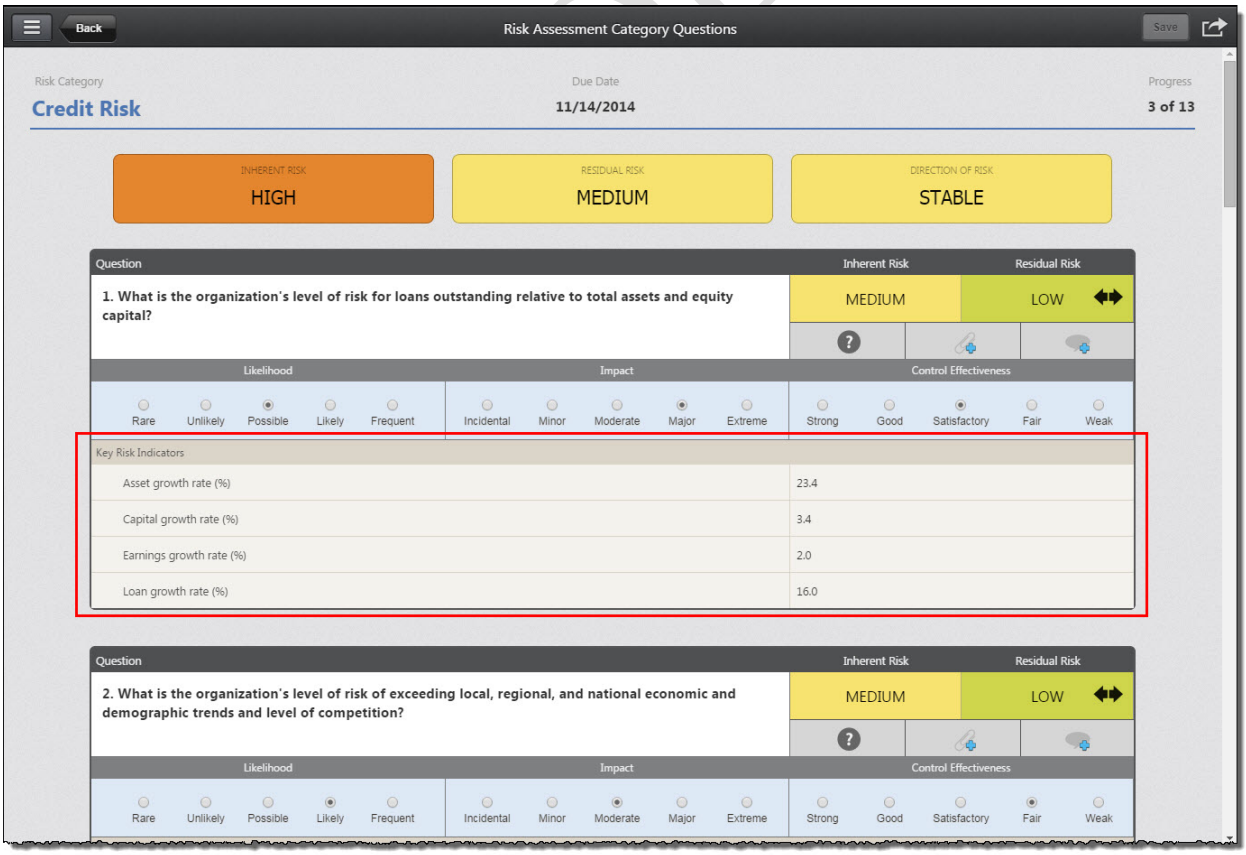


After you enter and save a value for the indicator, the Answered column on the KRI list will display a "Y" for Yes, indicating that the KRI value has been answered.

Key Risk Indicators on Assessments

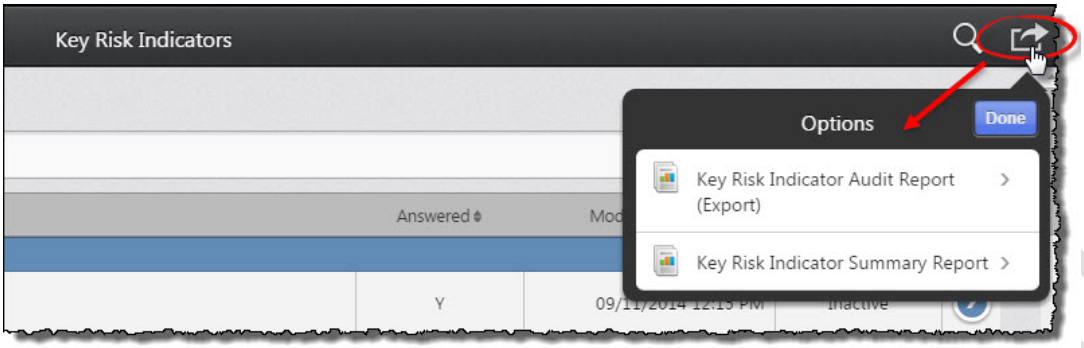
Key Risk Indicators that have been given a value and are marked to Show on Assessments will display on relevant assessment questions on Risk Assessments.

The indicators will display below each question, with the description and the value, to help qualify responses to the assessment questions and make the answers more objective.



Key Risk Indicator Reports

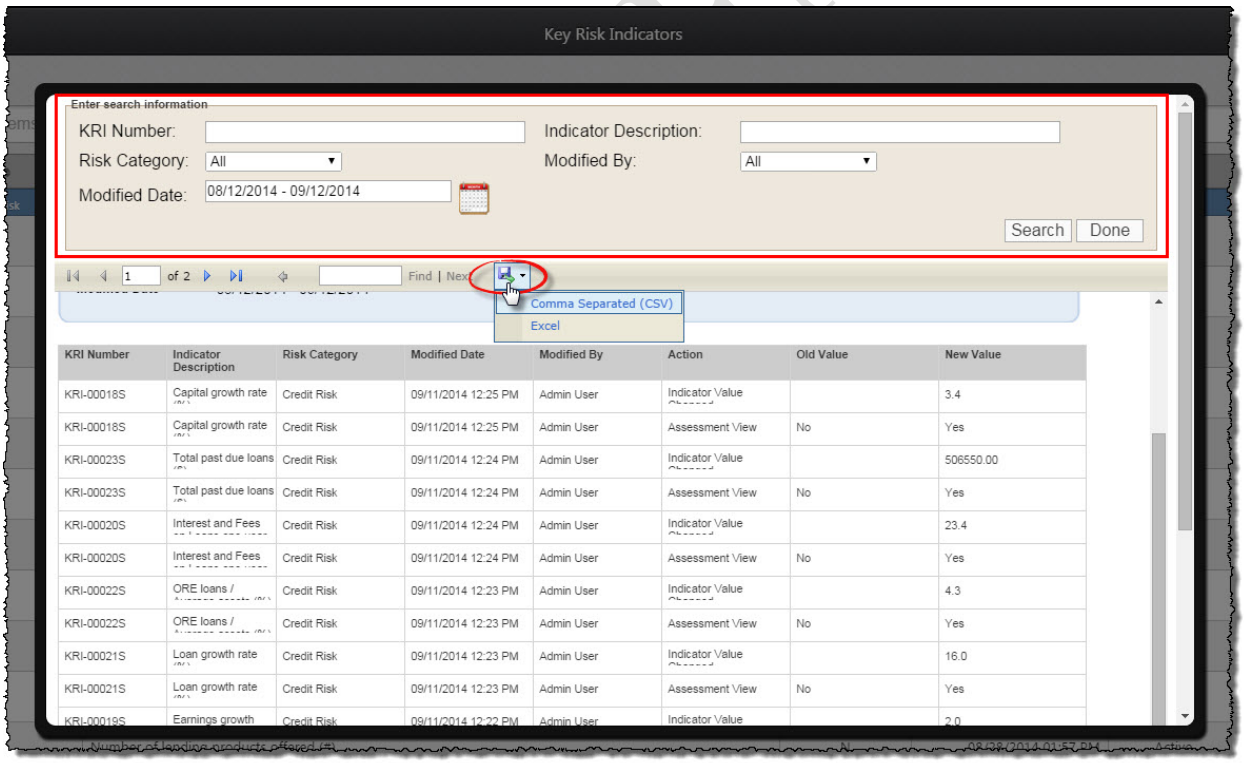
You can access a Key Risk Indicator Audit Report (Export) and a Key Risk Indicator Summary Report from the **Options** menu of the main Key Risk Indicators page.



Select the **Options** menu icon in the top right corner and select the desired report from the menu.

Key Risk Indicator Audit Report (Export)

This report provides a comprehensive list of all the changes that have been made to all indicators available in the system.



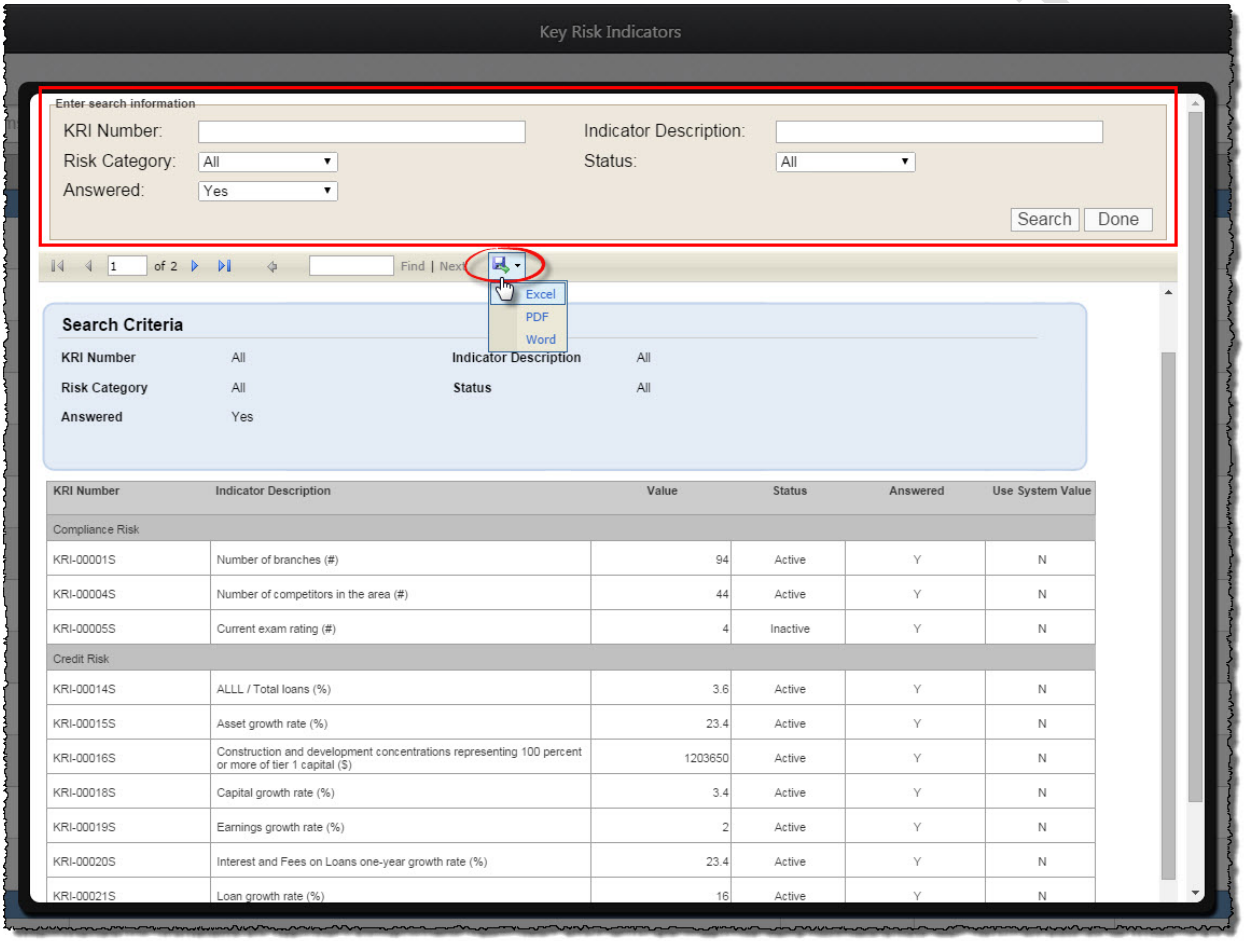
The report includes search criteria for KRI Number, Indicator Description, Risk Category, Modified Date and Modified By (user).

The report can be exported to a CSV or Excel file format.

The report contains columns for the KRI Number, Indicator Description, Risk Category, Modified Date, and Modified By. The report also includes the Action that was taken, i.e. a value was changed or the indicator was set to Inactive, along with the Old or previous Value and the New Value.

Key Risk Indicator Summary Report

This report provides a summary of all the indicators in the system. You can search the report by KRI Number, Indicator Description, Risk Category, Status and Answered values.

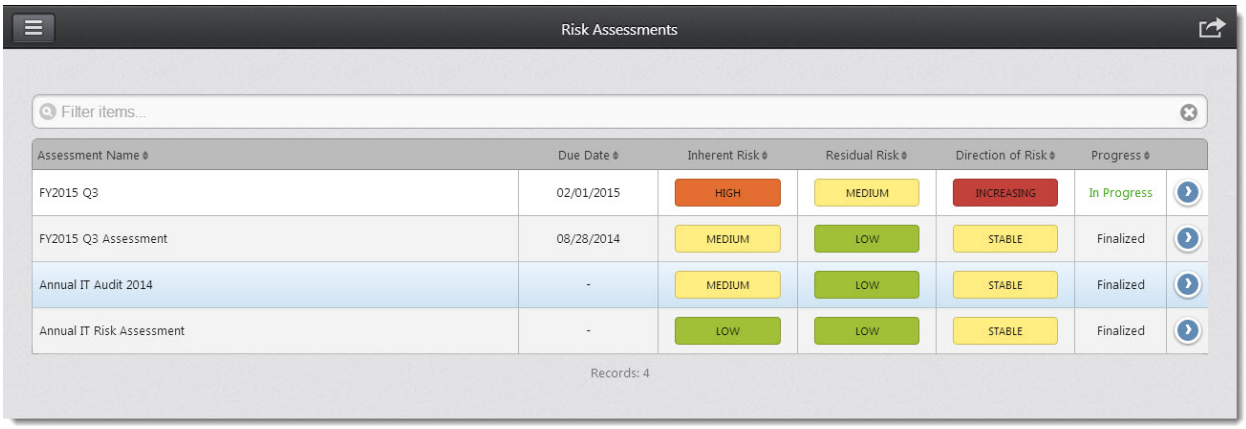

Key Risk Indicators
Enter search information
KRI Number:
Indicator Description:
Risk Category: All
Status: All
Answered: Yes
Search
Done
1 of 2
Find | Next
Excel
PDF
Word
Search Criteria
KRI Number All
Indicator Description All
Risk Category All
Status All
Answered Yes
KRI Number | Indicator Description | Value | Status | Answered | Use System Value
Compliance Risk
KRI-00001S | Number of branches (#) | 94 | Active | Y | N
KRI-00004S | Number of competitors in the area (#) | 44 | Active | Y | N
KRI-00005S | Current exam rating (#) | 4 | Inactive | Y | N
Credit Risk
KRI-00014S | ALLL / Total loans (%) | 3.6 | Active | Y | N
KRI-00015S | Asset growth rate (%) | 23.4 | Active | Y | N
KRI-00016S | Construction and development concentrations representing 100 percent or more of tier 1 capital ($) | 1203650 | Active | Y | N
KRI-00018S | Capital growth rate (%) | 3.4 | Active | Y | N
KRI-00019S | Earnings growth rate (%) | 2 | Active | Y | N
KRI-00020S | Interest and Fees on Loans one-year growth rate (%) | 23.4 | Active | Y | N
KRI-00021S | Loan growth rate (%) | 16 | Active | Y | N

The report output includes the KRI Number, the Indicator Description, the current Value, the indicator Status, whether the Value has been answered, and whether the Value is coming from the UBPR or provided by the user (Use System Value).

This report can be exported to Excel, PDF or Word file formats.

Risk Assessments

Select the **Risk Assessments** menu option from the SmartRisk IQ section of the main menu to access a list of your In Progress and Finalized Risk Assessments. This list will tell you the Name, the Due Date, the Inherent Risk level, the Residual Risk level, how your Direction of Risk is trending, and the Progress of each assessment.



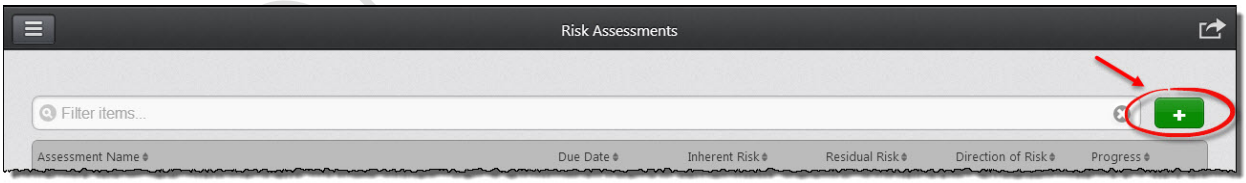
This list can be filtered by typing text in the Filter items search box to help you find a specific assessment.

You can access the details of a Risk Assessment by clicking the blue arrow on the far right side of the assessment row or anywhere in the row.

It is important to note that you can only have one Risk Assessment with a status of "In Progress" open at a time. Before you can begin a new Risk Assessment, you must complete and **Finalize** the previous one. Each time you finalize a Risk Assessment, you will be prompted to set a due date for the next assessment.

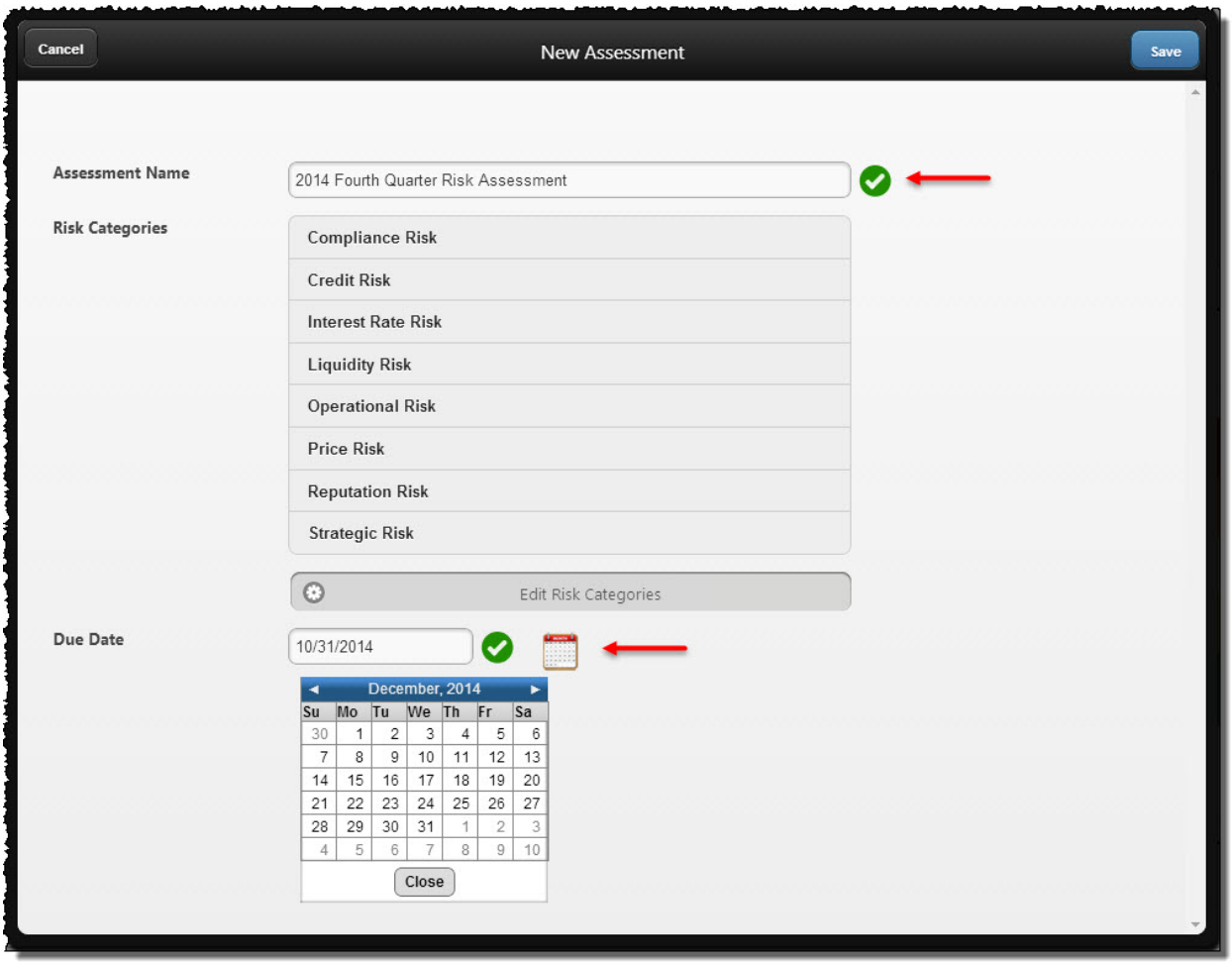
Create a New Risk Assessment

If you have not started an assessment yet, select the green plus button beside the Filter items search field on the Risk Assessment screen.



Important Note: The green plus button will only display if you have not created an assessment yet or if all your assessments are finalized.

CONFIDENTIAL



Once you've clicked the green plus button, a New Assessment pop-up window will display.

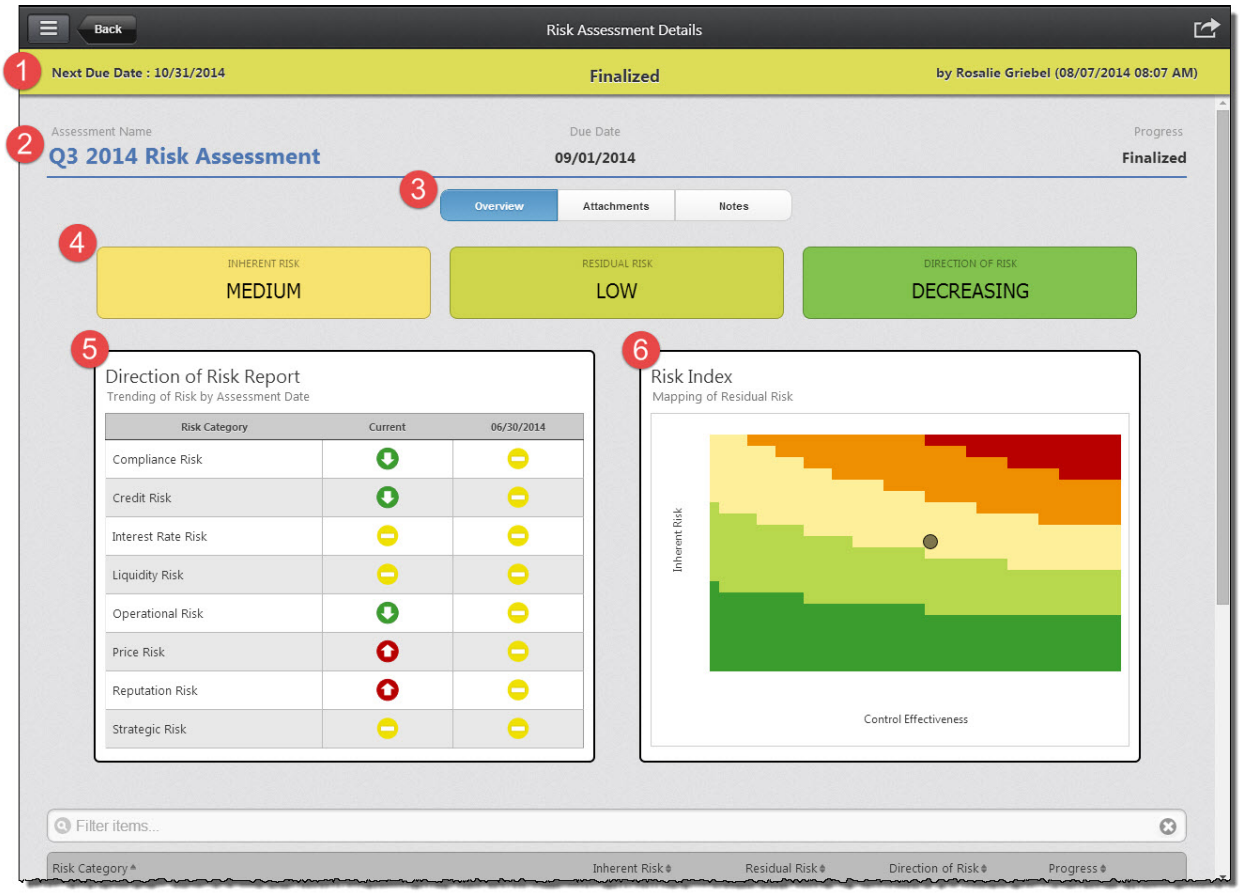
- Enter an Assessment Name to identify this assessment. This field is required.
- The Risk Categories contained in the assessment are currently locked and default to the eight system categories. In a future release you will be able to edit the categories included in your assessment, including the ability to add custom categories.
- Enter a Due Date on which the assessment will be due to be finalized. Use the calendar control to select a date or enter the date using your keyboard. The date must be entered in the proper format, mm/dd/yyyy. This field is required.

Save the assessment by selecting the **Save** button in the top right corner of the pop-up window. The Risk Assessment Details will display.

Risk Assessment Details

The Risk Assessment Details provides a significant amount of information about each assessment.

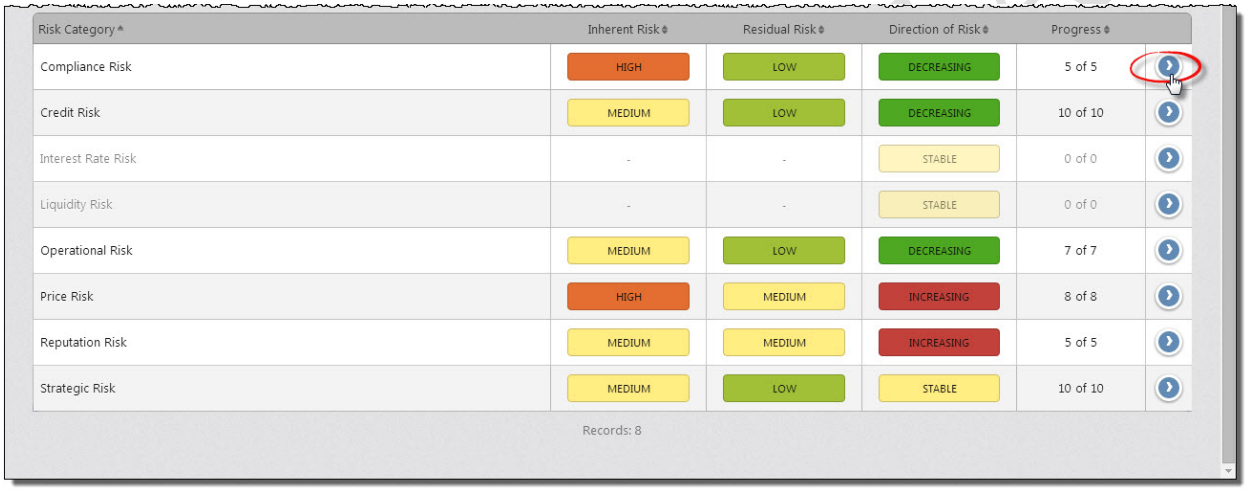
Let's break it down by section.



1. This section only displays on assessments that have been finalized. It shows the date on which the next assessment is due, which was established when the assessment was finalized; it shows that the assessment has been Finalized; and it shows the name of the user who finalized the assessment and the date/time it was finalized.
2. This section displays the Assessment Name, the current assessment due date, and the Progress (In Progress or Finalized).
3. These tabs allow you to switch from the Overview screen, to a list of all Attachments uploaded for this assessment, to a list of all Notes made for this assessment. Attachments and Notes are added at the question level. See Risk Assessment Category Questions for information about adding attachments and notes.
4. The Inherent Risk, Residual Risk, and Direction of Risk are automatically calculated by the system based on the responses to all the questions across all the Risk Categories in the assessment.
    - Inherent Risk calculates the level of risk your institution is subject to, based on the likelihood and impact of each question *before* your control effectiveness is considered.

- Residual Risk calculates the level of risk your institution is subject to, based on the likelihood and impact of each question *after* your control effectiveness has been considered.
- Direction of Risk calculates how your risk is trending from one assessment to the next. A change from a lower residual risk to a higher residual risk will constitute an increased direction of risk; a change from a higher residual risk to a lower residual risk will constitute a decreased direction of risk; and no change in residual risk will constitute a stable direction of risk.

5. The Direction of Risk Report trends the changes in the direction of risk from one assessment to the next, broken down by Risk Category. A column for each assessment with the date the assessment was finalized, including the current assessment, displays an up arrow, down arrow or dash icon to represent increased risk, decreased risk or stable risk, respectively.
6. The Risk Index report shows where the current assessment's residual risk lies on the risk spectrum (Very Low to Very High).



Risk Category	Inherent Risk	Residual Risk	Direction of Risk	Progress
Compliance Risk	HIGH	LOW	DECREASING	5 of 5
Credit Risk	MEDIUM	LOW	DECREASING	10 of 10
Interest Rate Risk	-	-	STABLE	0 of 0
Liquidity Risk	-	-	STABLE	0 of 0
Operational Risk	MEDIUM	LOW	DECREASING	7 of 7
Price Risk	HIGH	MEDIUM	INCREASING	8 of 8
Reputation Risk	MEDIUM	MEDIUM	INCREASING	5 of 5
Strategic Risk	MEDIUM	LOW	STABLE	10 of 10

Records: 8

The second half of the page lists each Risk Category, the risk levels by category, and the progress of questions completed per category.

Note that the risk assessment questionnaire is broken out by Risk Category – there is a different set of questions under each category. All questions must be answered or opted out of before an assessment can be finalized.

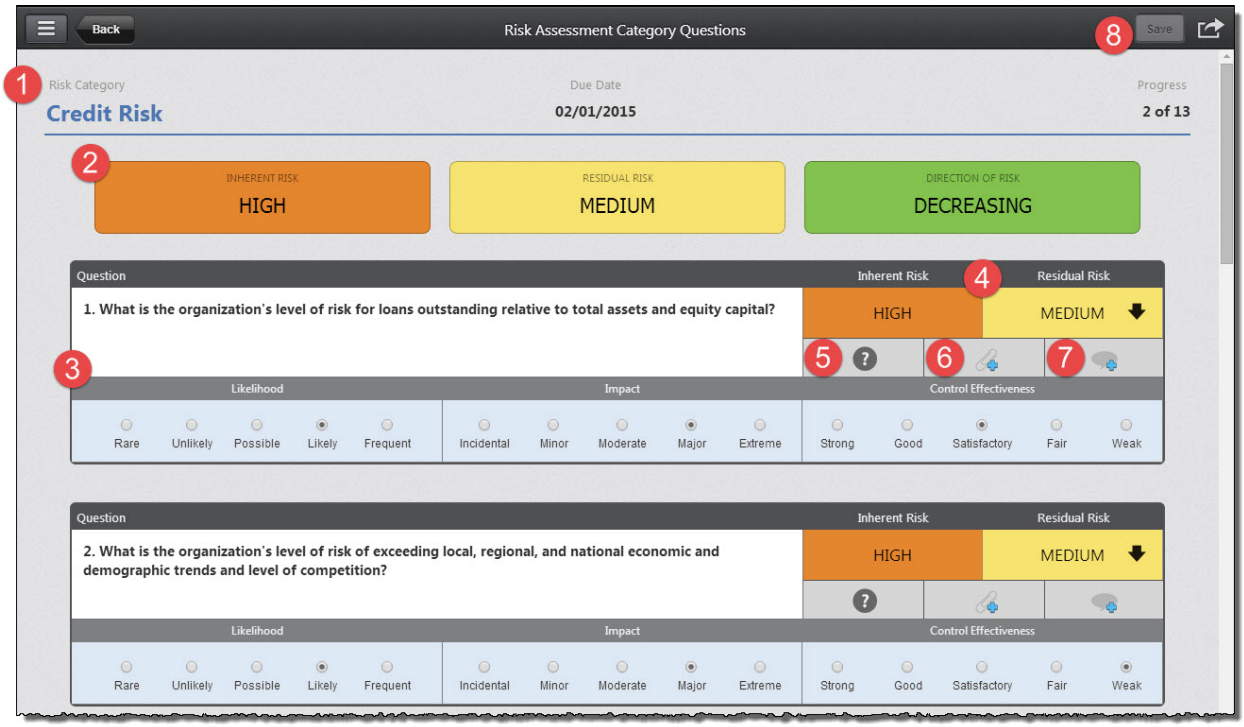
To access the questions for a category click on the arrow button, or anywhere in the row for the desired category.

CONFIDENTIAL

Risk Assessment Category Questions

As mentioned, there is a separate set of questions for each Risk Category. Each Category Questions page consists of several elements and features to help you complete the assessment.

Let's take a closer look.



1. Along the top of the page you will find the name of the Risk Category to which these questions belong, as well as the Due Date of the assessment and your progress, i.e. the count of questions you've completed versus the total number of questions for the category.
2. The Inherent Risk, Residual Risk, and Direction of Risk are automatically calculated by the system and apply specifically to the questions contained in the Risk Category. The calculations are the same as they are at the overall assessment level – Inherent Risk is the risk *before* control effectiveness is considered; Residual Risk is the risk *after* control effectiveness is considered; and Direction of Risk is the change, upward or downward, for the category since the last assessment.
3. Each question has three sections that must be completed:
    - Likelihood – Indicate the likelihood that this risk factor could occur during this assessment period at your institution. Your options are Rare, Unlikely, Possible, Likely, or Frequent.
    - Impact – Indicate the impact this risk factor will have on your institution during this assessment period. Your options are Incidental, Minor, Moderate, Major, or Extreme.
    - Control Effectiveness – Indicate the level of controls you already have in place at your institution to mitigate this risk factor during this assessment period. Your options are Strong, Good, Satisfactory, Fair, or Weak.

CONFI

4. Inherent Risk, Residual Risk, and Direction of Risk are also calculated per question, again based on the likelihood and impact before and after your controls are considered and the change in residual risk since the last time you answered this question.
5. Access Intelligent Content by clicking the question mark icon for each question. The information available here will help determine what your current Control Effectiveness should be.
6. Upload attachments specific to a question. Attachments could include supporting materials or other artifacts needed to justify a specific response to the question.
7. Add comments to support your responses to the question or notify other users viewing the assessment of important notes.
8. Make sure you save any responses, attachments, or comments you add before leaving the page.

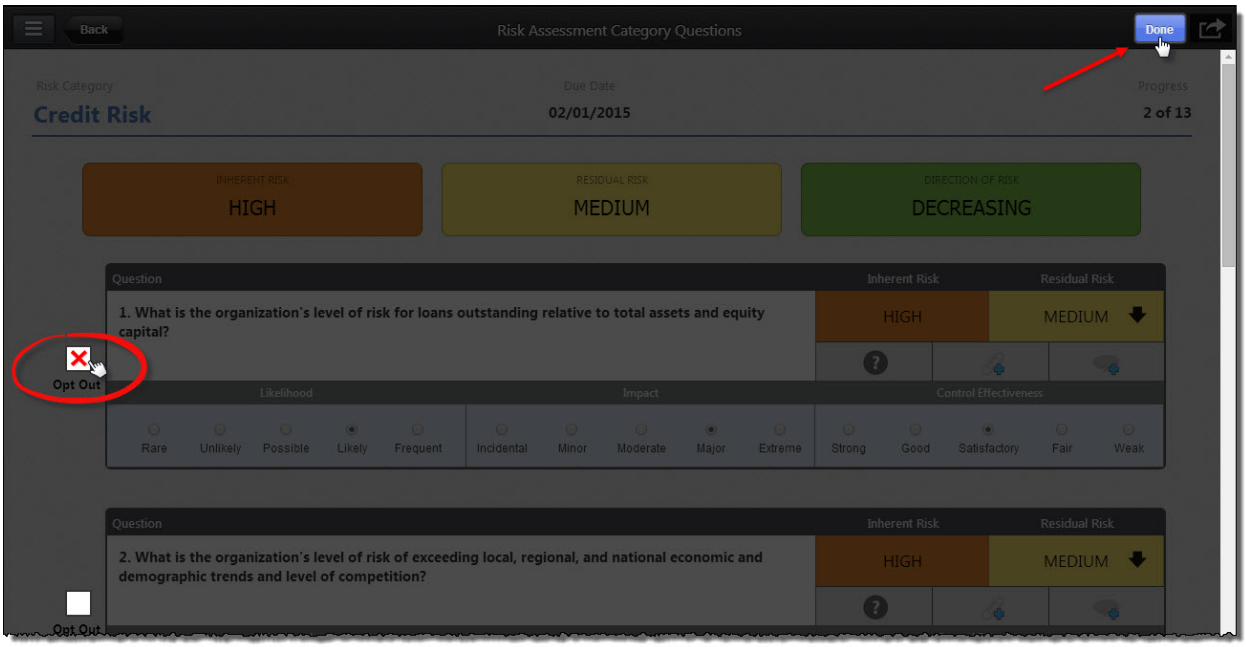
Opting Out of Questions

You have the ability to opt out of questions on the assessment. If you opt out of one or more questions, the selected questions will no longer display on the assessment and will not be counted or required as part of the risk calculation and assessment finalization.

To opt out of one or more questions, select the **Options** icon in the top right corner of the Risk Assessment Category Questions screen and select **Opt Out of Questions** from the menu.

The page will become grayed out (disabled) and a check box will appear beside each question.

CONFIDENTIAL



Click in the check box beside the question(s) you would like to opt out of and then select **Done** to save your selection(s).

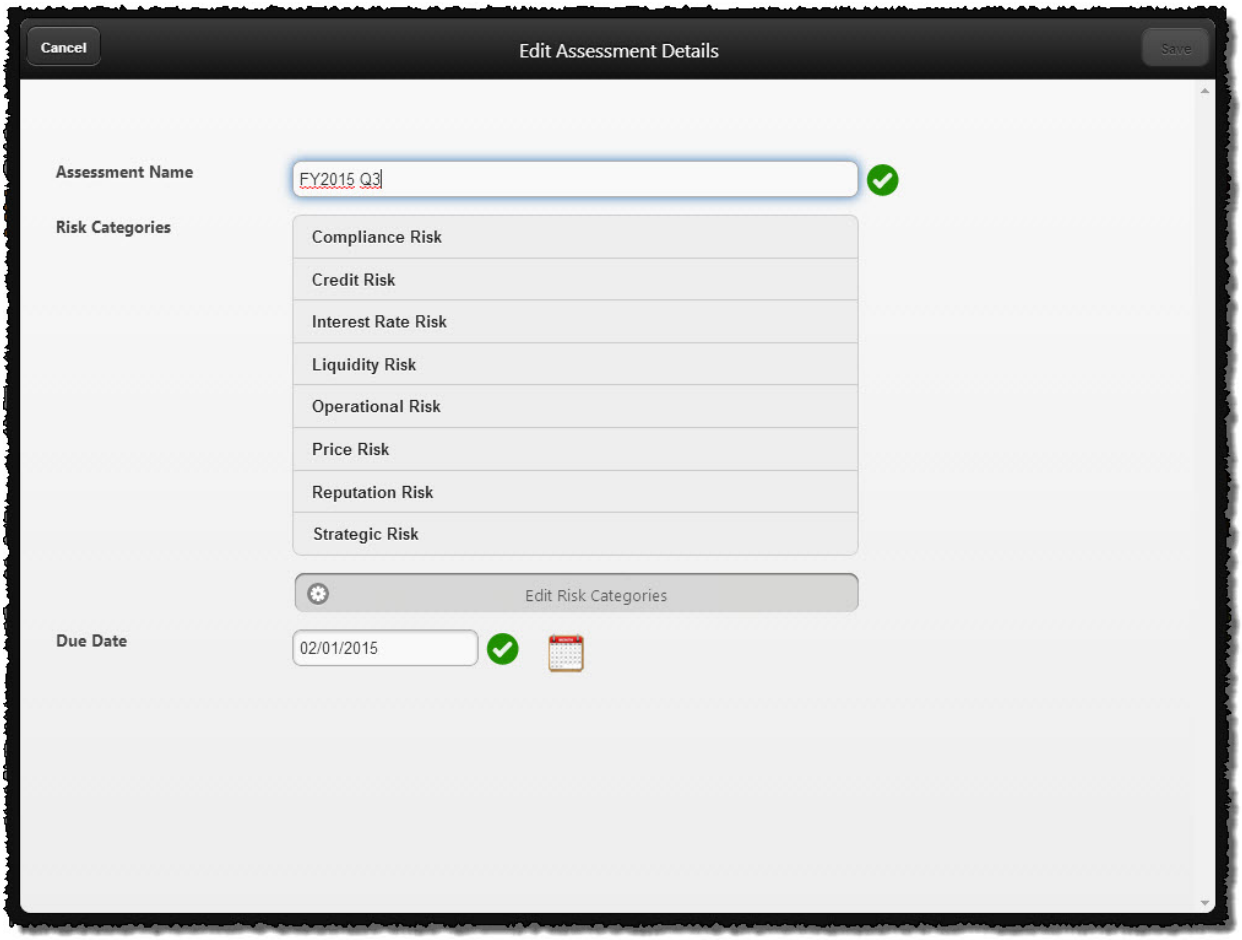
Any questions you choose to opt out of will no longer appear on the main Risk Assessment Category Questions screen. To opt *back in* to a question, select the **Opt Out of Questions** from the Options menu and *deselect* the Opt Out check box for the desired question(s), then select **Done**.

Note that the question numbers *never* change, so if you have opted out of any questions the question numbers will skip.

Edit Assessment Details

To change the name of the assessment or the due date, go to the **Options** menu on the Risk Assessment Details and select **Edit Assessment Details**.

A pop-up screen will appear that allows you to edit the name and the due date. Be sure to **Save** before exiting the window.



Finalize Assessment

Once you have completed all the questions for each Risk Category on the assessment you can finalize the assessment. Finalizing the assessment will lock all the responses and supplemental information (attachments and comments) – the assessment cannot be edited once it is finalized.

To finalize an assessment, go to the **Options** menu on the Risk Assessment Details and select **Finalize Assessment**.

Note that you cannot finalize an assessment until all questions have been answered or opted out of. The **Finalize Assessment** option will remain grayed out until the assessment has been completed.

Risk Calculations

The method used to calculate your Risk on each assessment is relatively simple.

As described previously, each question, category, and assessment has an Inherent Risk score and a Residual Risk score. Inherent Risk is based on the Likelihood and Impact of each risk factor *before* your Control Effectiveness is considered, and Residual Risk is based on the Likelihood and Impact of each risk factor *after* your Control Effectiveness is considered.

Assessment Question Risk Levels

Likelihood is measured using the following potential responses, where each response is equally weighted and given a point value of 1 – 5.

- Rare = 1 point
- Unlikely = 2 points
- Possible = 3 points
- Likely = 4 points
- Frequent = 5 points

Impact is measured the same way, using the following potential responses, where each response is equally weighted and given a point value of 1 – 5.

- Incidental = 1 point
- Minor = 2 points
- Moderate = 3 points
- Major = 4 points
- Extreme = 5 points

The actual Risk levels given to both Inherent and Residual Risk represent a percent value range. The Risk levels and their associated percent ranges are:

- Very Low = 0% - 20%
- Low = 21% - 40%
- Medium = 41% - 60%
- High = 61% - 80%
- Very High > 81%

For Inherent Risk, the percentage is calculated by multiplying the Likelihood and Impact scores and dividing that by the maximum points available, that being 25 points.

For example, you respond on a question that your Likelihood that the risk factor will occur is Possible, so you receive 3 out of 5 points for Likelihood. You respond that the Impact of the risk factor is Major, so you receive 4 out of 5 points for Impact.
The formula then becomes:

(3 points for Likelihood × 4 points for Impact) ÷ 25 maximum points = .48 or 48%

This gives you an Inherent Risk of Medium.

CONFIDENTIAL

To calculate the **Residual Risk**, the Inherent Risk score is multiplied by the Control Effectiveness, which simply consists of weighted values based on the response.

- Strong = .525
- Good = .625
- Satisfactory = .725
- Fair = .825
- Weak = .925

The **Residual Risk** is calculated by multiplying the Inherent Risk score by the Control Effectiveness value based on the response given on the question. The higher the Control Effectiveness, the more your Inherent Risk is mitigated, and therefore, the lower your Residual Risk percentage.

For example, if your Inherent Risk is 48% (Medium) and your Control Effectiveness is Good (.625), your Residual Risk would be 30% or Low.

Inherent Risk .48 × Control Effectiveness .625 = .30 or 30% Low Residual Risk

So even though the Inherent Risk might be Medium, if you have good controls in place your Residual Risk is reduced to Low.

Category Risk Levels

At the Risk Category level, the Inherent and Residual Risk scores are simply the average percentages for all the questions that have been answered.

Assessment Risk Levels

The Assessment Inherent and Residual Risk scores are also the average percentages of all the Risk Category scores in which the Risk Category has at least one completed question.

A completed, answered question is one that has a Likelihood and Impact response selected and saved. If no Control Effectiveness has been selected, it is assumed to be 0% for the purposes of the Residual Risk calculation. Once a Control Effectiveness response is saved, the Residual Risk will update.

SmartRisk IQ Reporting

There are several reporting options within the SmartRisk IQ area of Elite. Reporting is generally divided into three categories: Audit Reporting, Detail Reporting and Summary Reporting.

All reports can be accessed via the **Options** menus either on the Risk Assessment Details or the Risk Assessments main page.

Risk Assessment Detail Report

To access a detailed, printable report that includes all the questions, responses, attachment names, comments, and risk ratings at the assessment and question levels across all Risk Categories for an assessment, go to the **Options** menu on the Risk Assessment Details and select **Risk Assessment Detail Report**.

CONFIDENTIAL

This report provides a formatted, printable version of the assessment that includes the overall Inherent Risk, Residual Risk, and Direction of Risk for the assessment as well as a detailed view of each question on the assessment grouped by Risk Category.

The report can be exported to Excel or PDF.

Assessment Audit Report

Access the Assessment Audit Report from the Options menu on the main Risk Assessments grid page.

The Assessment Audit Report (Export) provides a detailed list of every change made on all risk assessments or a specific assessment for audit purposes.

The report can be exported to CSV or Excel.

Assessment Executive Report

Access the Assessment Executive Report from the Options menu on the main Risk Assessments grid page.

The Assessment Executive Report provides a summary-level overview of assessment activity over the previous rolling 12 months. All finalized assessments within the period are reflected in the report, which includes risk trending charts and tables at an overall level as well as a break down by Risk Category.

Assessment Question Detail Report

Access the Assessment Question Detail Report from the Options menu on the main Risk Assessments grid page.

The Assessment Question Detail Report is another way to view all the questions on assessments with the responses provided as well as the risk ratings, information about Opt Out selections, comments and attachments. This version of the Question Detail is presented in a table view and is exportable to CSV or Excel, making it easy to conduct additional analysis or even import into other systems.

The report can be exported to CSV or Excel.

Assessment Summary Report

Access the Assessment Summary Report from the Options menu on the main Risk Assessments grid page.

The Assessment Summary Report is essentially a printable version of the Risk Assessments grid page, which lists all the assessments you have finalized and in progress with the Due Date, Inherent Risk, Residual Risk, Direction of Risk, and Progress or status for each assessment.

This report can be exported to Excel, PDF, or Word.

Risk Appetite Trend Report

Access the Risk Appetite Trend Report from the Options menu on the main Risk Assessments grid page.

The Risk Appetite Trend Report compares the risk tolerance or appetite you set for each Risk Category in the Risk Management Settings to your actual Residual Risk on each assessment.

CONFIDENTIAL

This allows you to clearly identify where your risk is higher than your appetite, telling you where you might need stronger controls, and where your risk is lower than your appetite, telling you where you might be able to accept additional risk.

This report can be exported to Excel, PDF, or Word.

This completes the SmartRisk IQ section.

CONFIDENTIAL

Vendor Management Overview

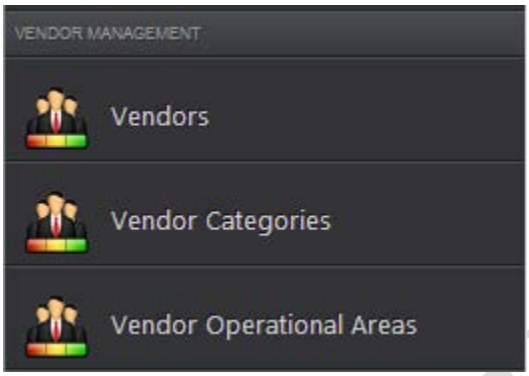
This section of the Elite Quick Start guide details the steps to create and manage Vendor Categories, Vendor Operational Areas, and create Vendors and the associated assessments.

Important Note: This guide is written with the assumption that all roles and users have been defined and created within the application. Please see Chapter 11 in the full user manual, which can be accessed via the Product Documentation link in the Navigation toolbar, for a more detailed explanation of all functions and reports as well as the functions required to access the features and functionality.

Navigation:

Most of the navigation within the application is driven through the left side Navigation toolbar.

Only those links which the user has access to via security functions will be available in the Navigation toolbar. For Vendor Management, the section will be displayed as:



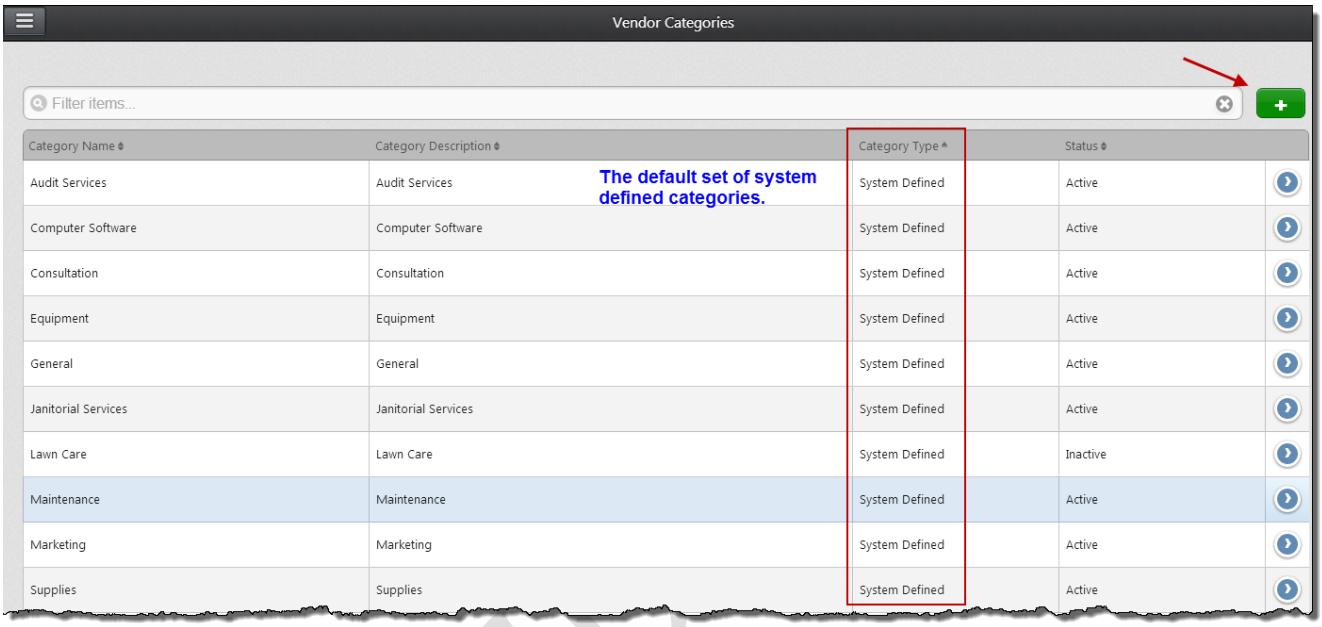
CONFIDENTIAL

Vendor Categories – Create and Manage

Categories classify vendors based on the service that they provide to your institution.

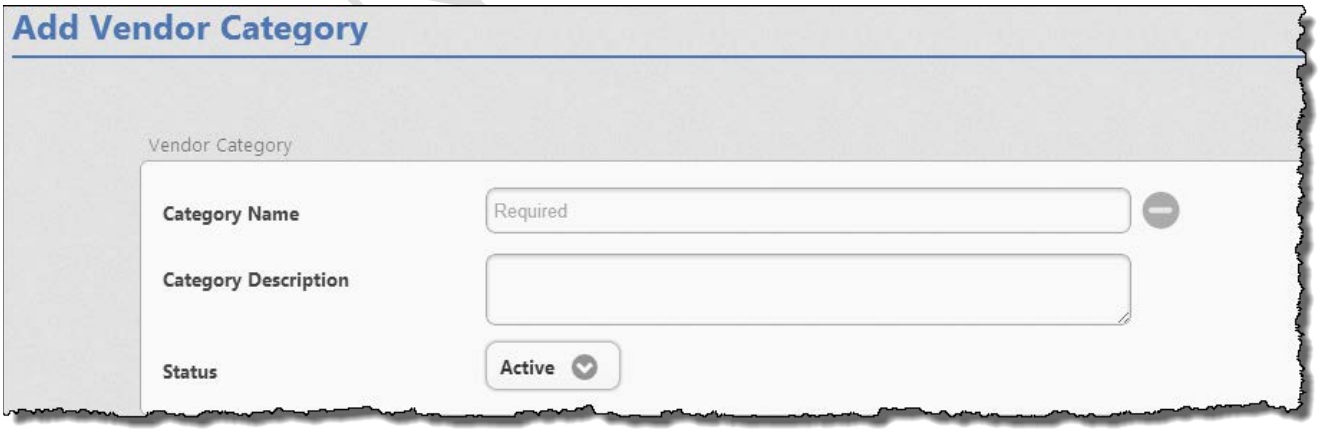
By default, there are a set of system defined categories; however, your institution may elect to create additional categories and/or deactivate system defined categories that will not be used by your institution.

1. Select the **Vendor Categories** link. The Vendor Category list will display.



Category Name	Category Description	Category Type	Status
Audit Services	Audit Services	System Defined	Active
Computer Software	Computer Software	System Defined	Active
Consultation	Consultation	System Defined	Active
Equipment	Equipment	System Defined	Active
General	General	System Defined	Active
Janitorial Services	Janitorial Services	System Defined	Active
Lawn Care	Lawn Care	System Defined	Inactive
Maintenance	Maintenance	System Defined	Active
Marketing	Marketing	System Defined	Active
Supplies	Supplies	System Defined	Active

2. To create a new vendor category, click on the plus sign. The Vendor Category Details page will display.
3. The **Category Name** is required. The description is optional and by default, the Status is set to Active. Make any necessary changes.



- Category Name
  - The category name is required to create a category. The category name must be unique within the client. This field can contain a maximum of 50 alphanumeric characters.
- Category Description

- This field can contain a maximum of 100 alphanumeric characters.

- Status
  - This field will be a drop down with the option to select a status of active or inactive. The default will be set to active.
  - An inactive category will not be available for assignment to a vendor. Inactive categories can be reactivated.
    Important Note: A system defined category can be set to inactive if your institution does not use.

4. The **Save** button will be enabled once a Category Name is chosen. You can return to the category detail page to make changes at any time. When the Save button is clicked a message will be displayed: Vendor Category successfully saved. Would you like to create a new item or return to the grid?'

Confirmation
Vendor Category successfully saved. Would you like to create a new category or return to the grid?
Create New Category
Back to Grid

- Clicking *'Create New Category'* will give the user the ability to create a new category.
- Clicking *'Back to Grid'* will direct the user back to the Vendor Categories page to view the newly created category in the list.

If a user tries to navigate away from the Category Details page without saving, the following message will appear: 'You have unsaved changes. Are you sure you want to leave the page?'

- Clicking *'Ok'* will allow the user to leave the page and discard any changes made.
- Clicking *'Cancel'* will keep the user on the current page.

Important Note: Categories cannot be deleted.

Editing a Vendor Category

A custom added category can be edited at any time. With the exception of the category type, all other category fields are editable. To retain changes select the **Save** button prior to leaving the Category Detail Page.

Important Note: Only the Status field is editable for the system defined categories.

CONFIDENTIAL

Vendor Operational Areas – Create and Manage

In this section, we will discuss how to create and modify operational areas to be assigned to vendors. Operational Areas are a way to identify the internal departments that are affected by the services (categories) provided by the vendor. Operational Areas are used with categories to organize the vendors and their associated services.

Creating an Operational Area

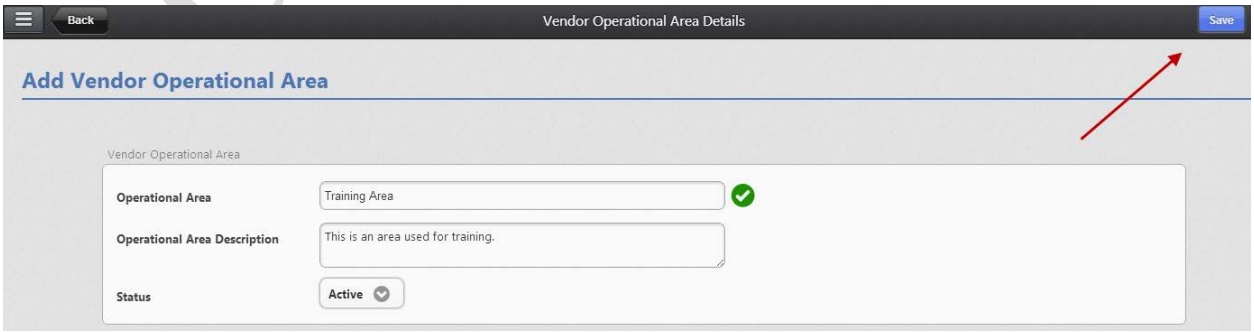
By default, there are a set of system defined operational areas; however, your institution may elect to create additional areas. System defined areas can be deactivated; otherwise, these cannot be edited. Inactive areas can be reactivated.

1. Select the **Vendor Operational Areas** link. The Vendor Operational Areas list will display.
2. To create an operational area, a user must click on the plus sign.

3. The Operational Area field is required to create an area.

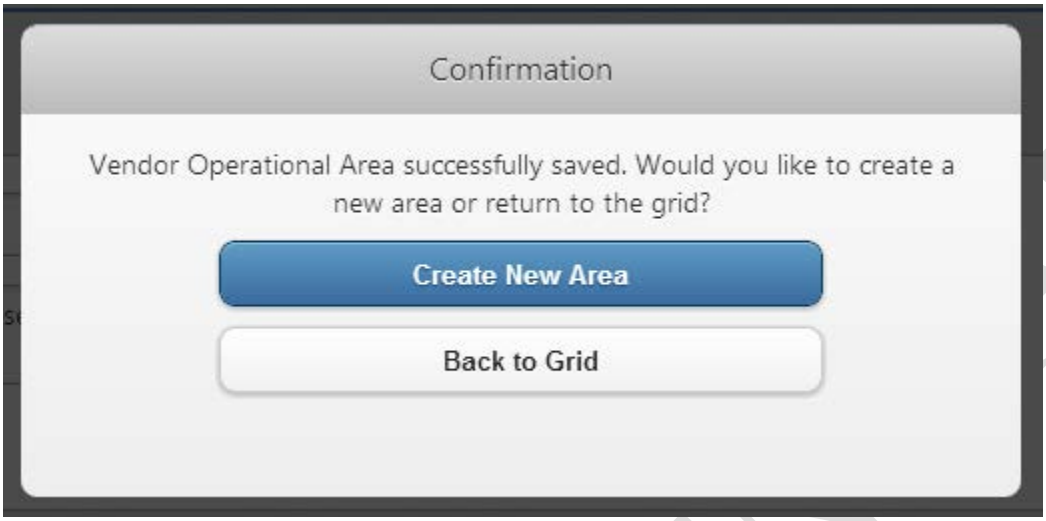
- Operational Area
  - The category name is required to create a category. The category name must be unique within the client. This field can contain a maximum of 50 alphanumeric characters.
- Operational Area Description
  - This field can contain a maximum of 100 alphanumeric characters.
- Status
  - This field will be a drop down with the option to select a status of active or inactive. The default will be set to active.
  - An inactive operational area will not be available for assignment to a vendor. Inactive operational area can be reactivated.

    Important Note: A system defined operational area can be set to inactive if your institution does not use.



CONFIDENTIAL

4. Once the required fields have been completed the 'Save' button will be enabled. Clicking '**Save**' will prompt the user with a confirmation of the save and provide two options for the user to choose from: Create New Area or Back to Grid. These options will only appear for the initial save of the area.


Confirmation
Vendor Operational Area successfully saved. Would you like to create a new area or return to the grid?
Create New Area
Back to Grid

In the next section, you will learn how to create and manage vendors.

Vendors – Create and Manage

Create and manage the Vendor Demographics

1. Select the **Vendors** link. The Vendors list will display.
2. To create a vendor, select the plus sign.
3. The Vendor Details page will display.

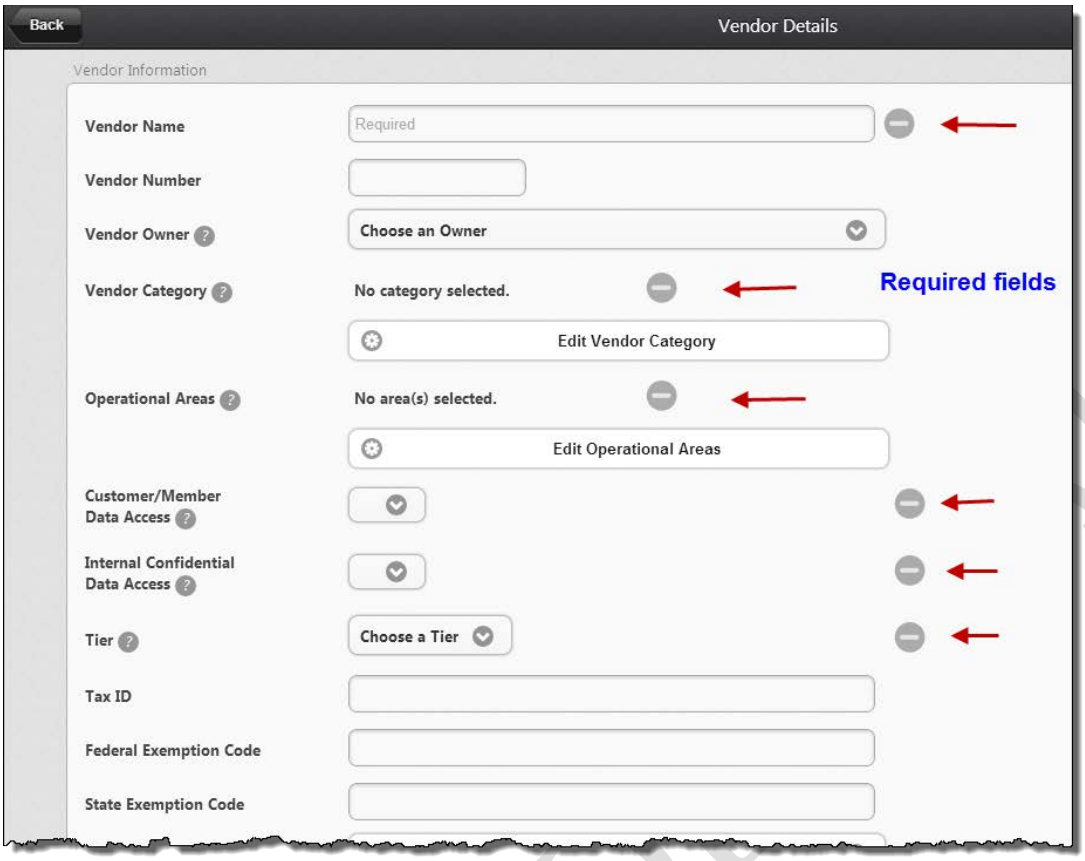
   Following is an explanation of the various field associated icons:

= Required field

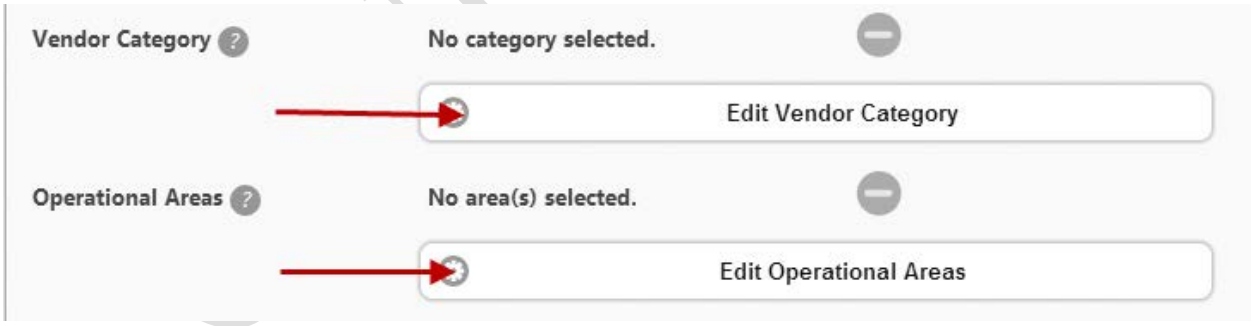
= Intelligent Content (or Help)

Important Note: Where applicable, review the intelligent content that is associated to applicable required fields prior to making a selection as an explanation for those fields are not provided in this document.

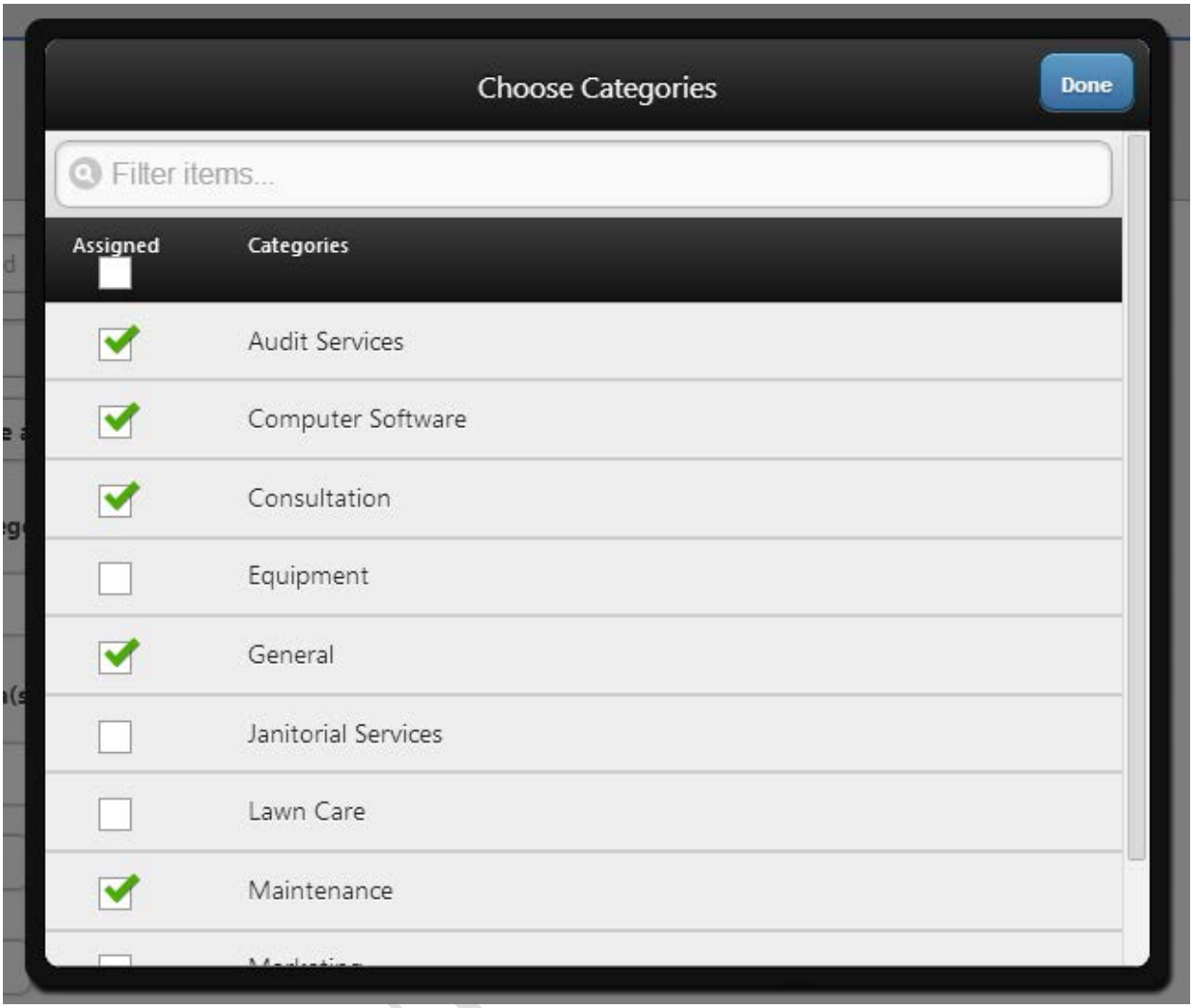
CONFIDENTIAL



4. At a minimum, populate the required fields.
5. To select a category and operational area, select the applicable button to display the list of available categories and areas.



6. To assign vendor categories to the vendor, select the **Edit Vendor Category** button.
7. Click on the checkbox next to the applicable categories. If all categories apply, select the checkbox under Assigned.



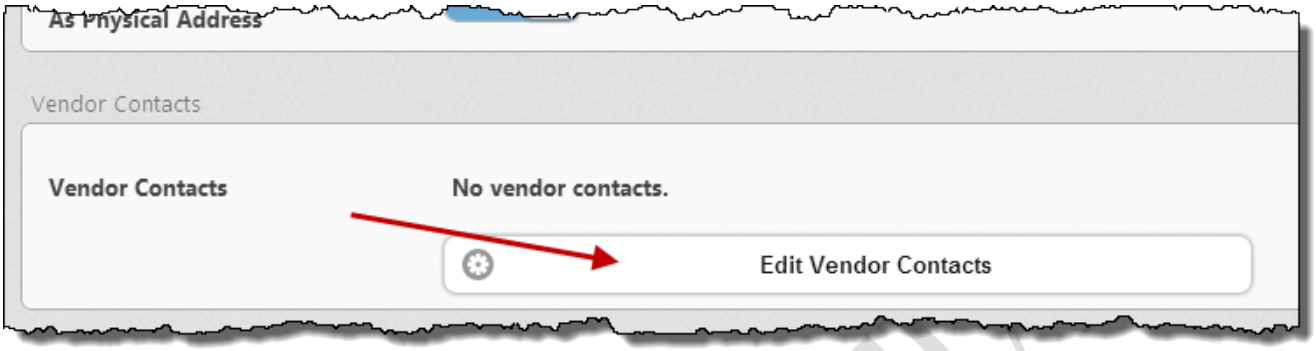
8. Then, select the **Done** button to accept the selections and return to the details page.
9. Repeat these steps to assign operational areas.
10. Upon supplying data for the required fields, the vendor can be saved to the database by selecting the **Save** button in the top right of the page.
11. Upon saving the vendor, options will be provided to stay on the vendor page or return to the vendor list page. Let's elect to stay on the page to continue building out the vendor information.

CONFIDENTIAL

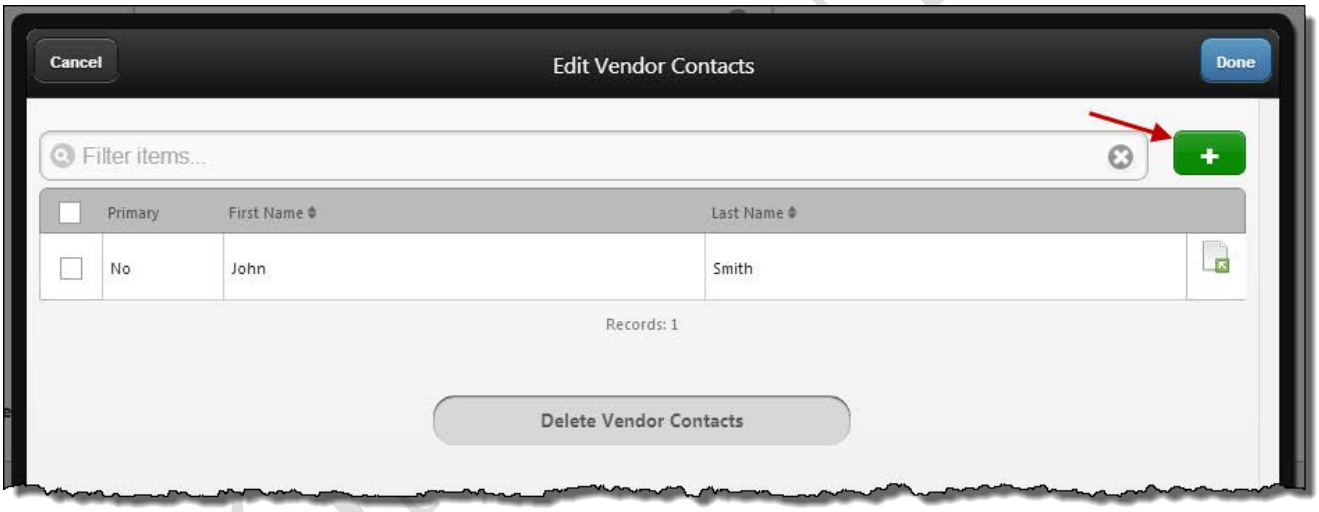
Add Vendor Contacts

Contacts can be optionally added to the vendor at any time.

1. Prior to or upon the initial creation of a vendor, select the **Edit Vendor Contacts** button.

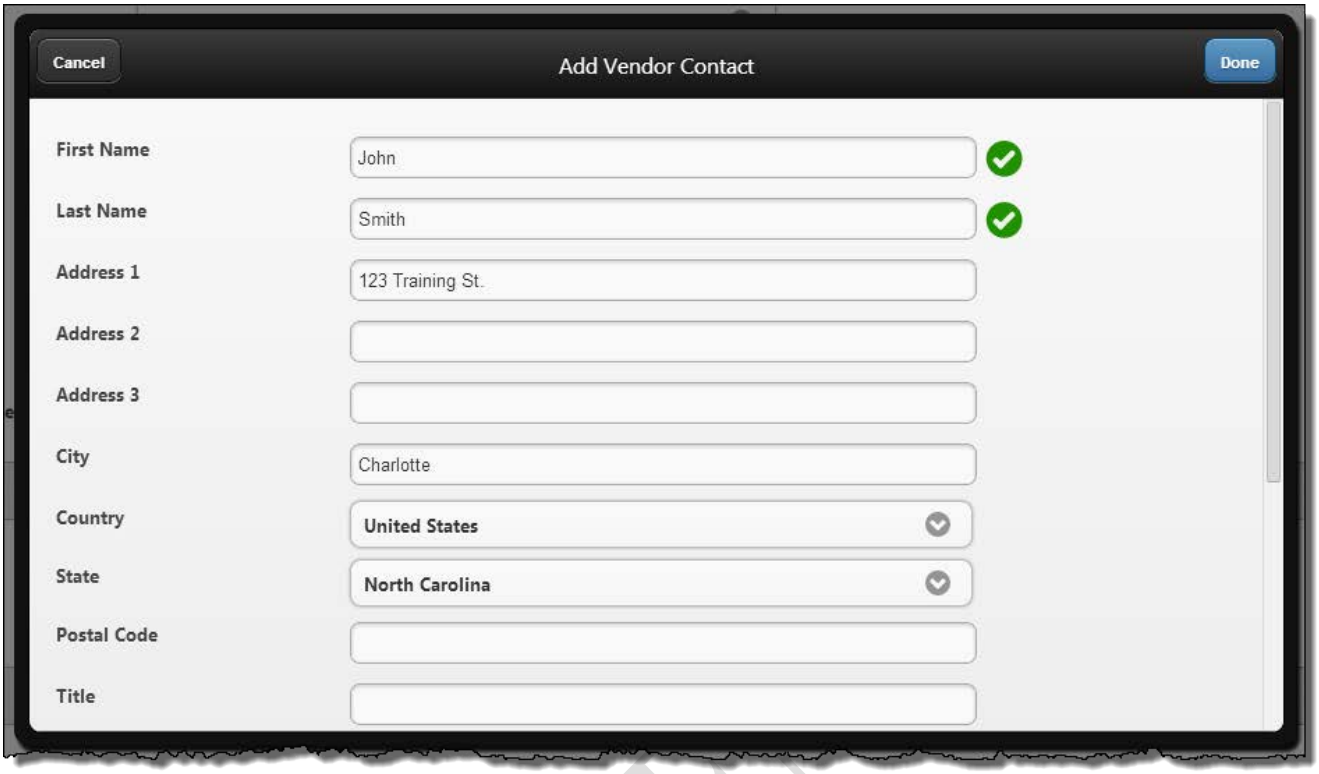


2. Select the plus sign to create additional contacts or select the **Done** button to return to the vendor details page.



3. The first and last names are required.

CONFIDENTIAL

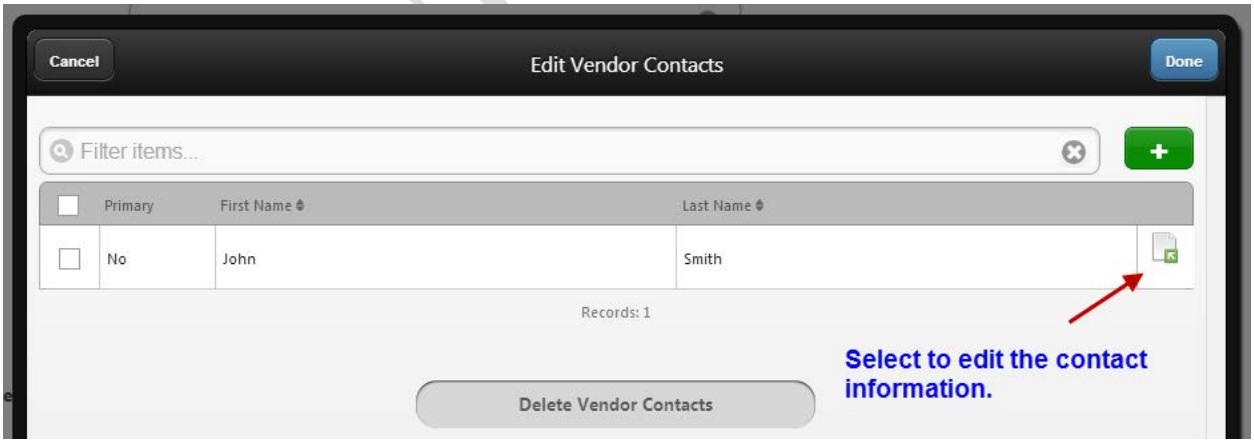


4. Upon providing all the applicable information, select the **Done** button to return to the Edit Vendor Contacts page.

   Note: only one contact can be set as the primary contact.

Edit Contact Information

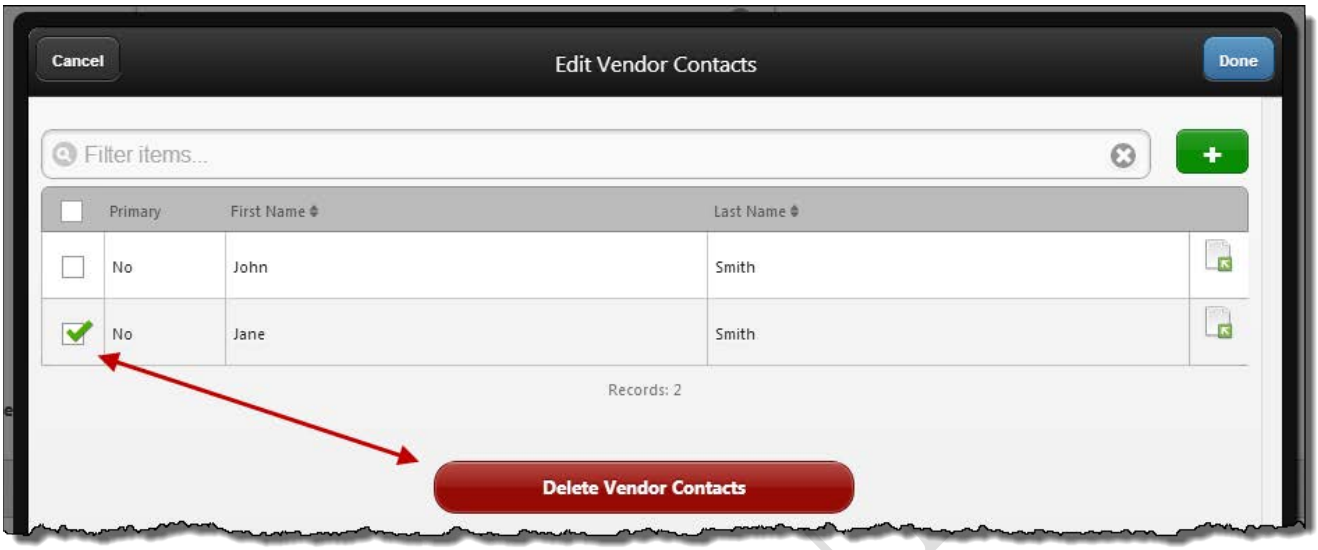
1. Existing contact information can be edited by selecting the edit icon (see image below).



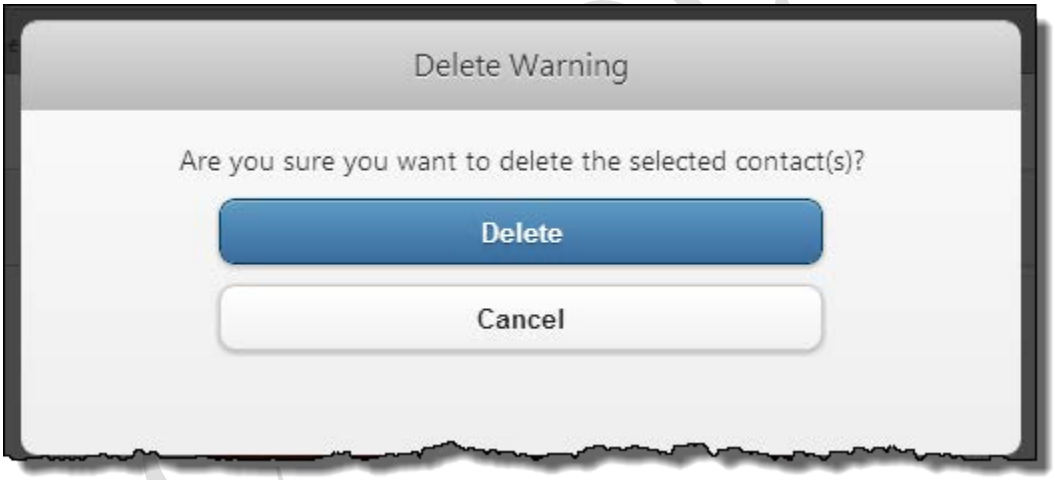
2. Edit the applicable information and click on the **Done** button to return to the Edit Vendor Contacts page.
3. When completed, select the **Done** button to return to the vendor details page.

Delete a Contact

1. From the Edit Vendor Contacts page, select the checkbox next to the contact that is to be deleted (see following image).



2. Select the **Delete Vendor Contacts** button. A warning will be displayed.

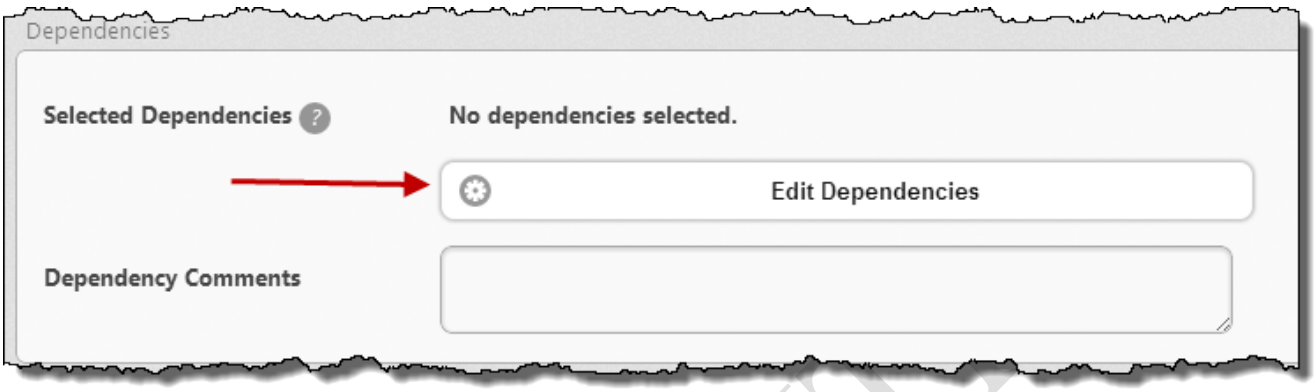


3. Select **Delete** to remove the contact. A deleted contact cannot be retrieved.
4. Select the **Done** button to return to the vendor details page.

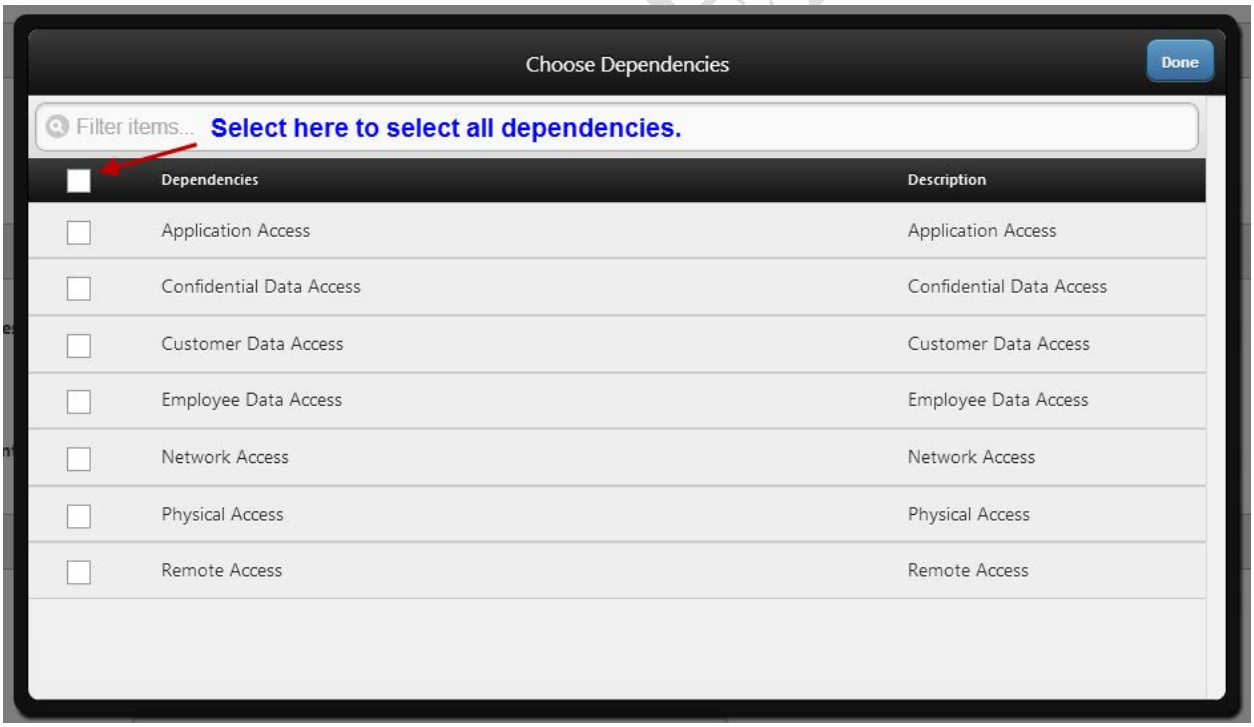
Assign Dependencies

A set of system defined dependencies (another service level provided by the vendor) are available for assignment to the vendor. New dependencies cannot be added.

1. Prior to or upon the initial creation of a vendor, select the **Edit Dependencies** button.



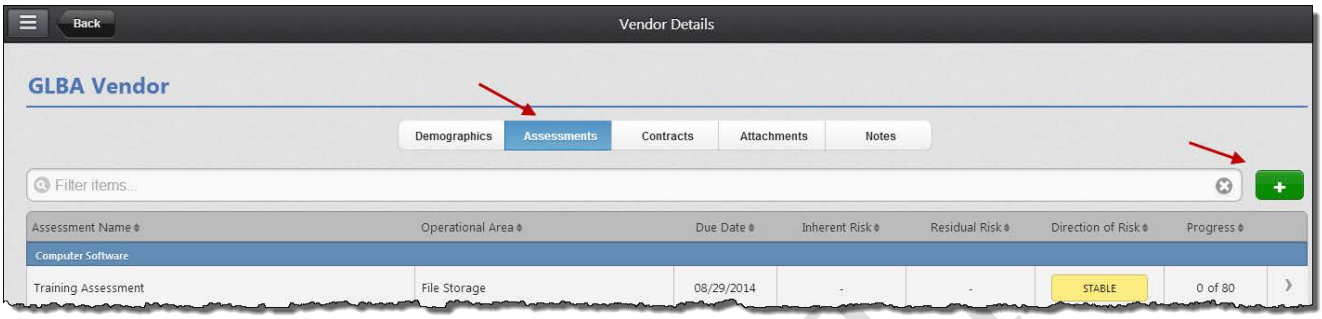
2. Select the checkbox next to the applicable dependencies or select the checkbox in the header to select all.



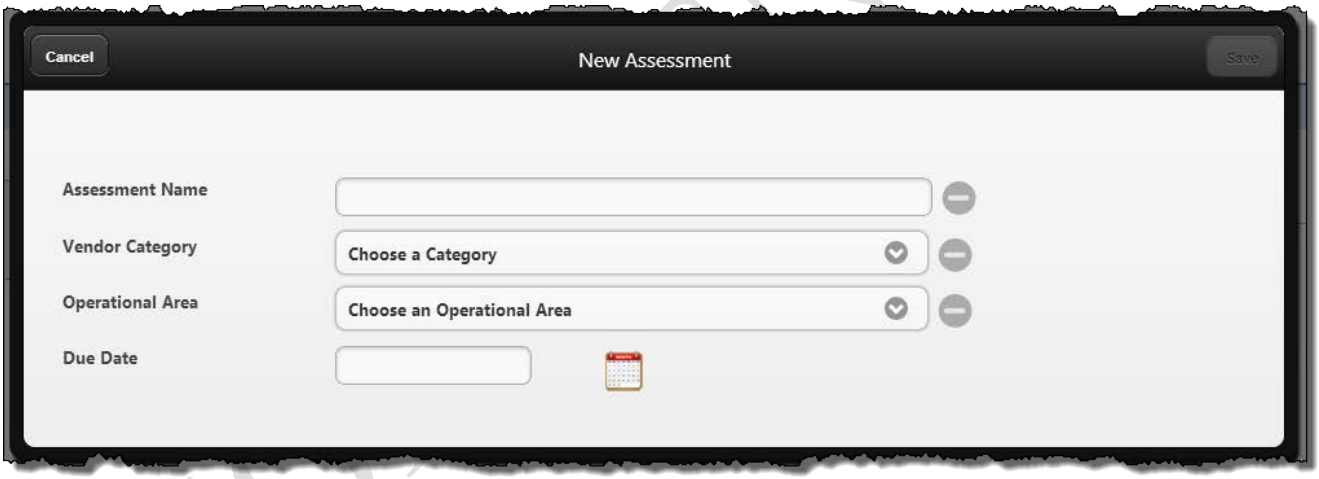
3. Select the **Done** button to return to the vendor details page.
4. From the vendor details page, select the **Save** button to retain all data.
5. To return to the Vendors list page, select the application **Back** button (not the browser Back button).

Vendor Assessments – Create and Manage

1. From the Vendors list page, select the vendor to create the assessment.
2. From the Vendor Details page, select the **Assessments** tab.
3. From the Assessments tab, select the plus sign.



The New Assessment page will display with three required fields.

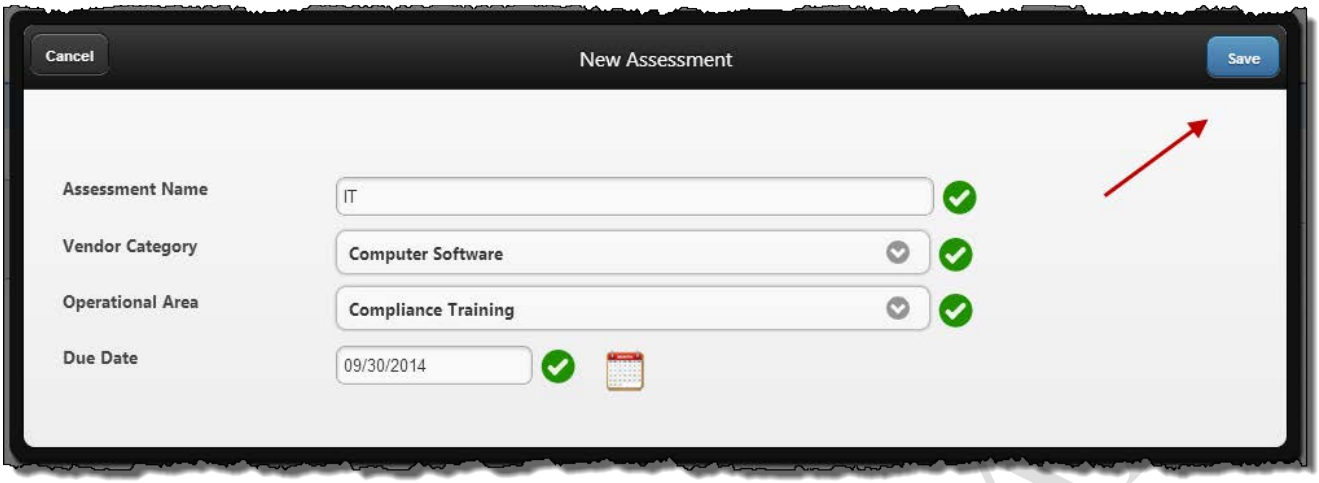


4. Provide an Assessment Name. The name must be unique to the vendor and a maximum of 100 alphanumeric characters.

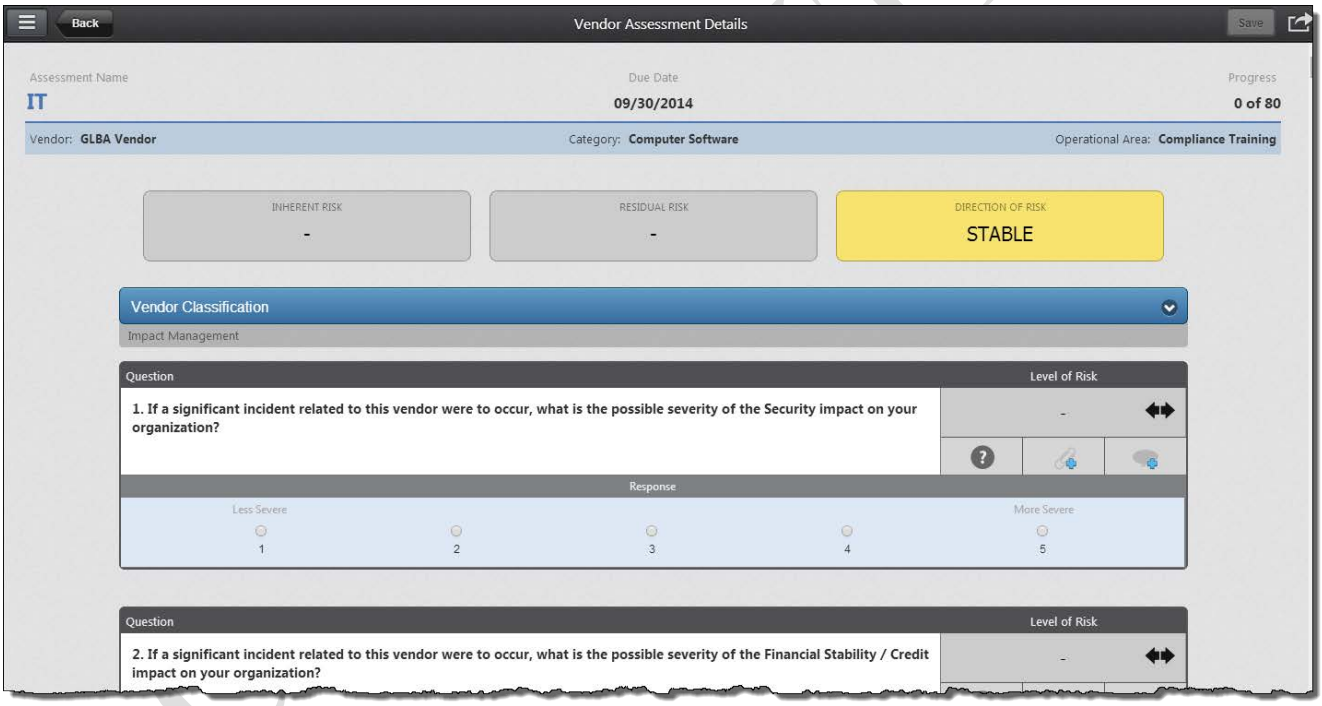
   Important Note: Only one assessment per Category/Operational Area combination can be open at a time.

5. Select a **Vendor Category** and **Operational Area** from the dropdown menus.
6. The Due Date can be populated upon the creation of the assessment or at a later time; however, it must be populated before finalizing the assessment.
7. Upon populating the required fields, the **Save** button will be enabled.

CONFIDENTIAL



8. Select the **Save** button create the assessment and advance to the Assessment Details page.



Introduction to the Assessment Details page

The Assessment Details page is made up of 80 questions that are broken down into the following sections:

- Vendor Classification
- Due Diligence
- High Risk

The questions/answers in the Vendor Classification section are related to determining the inherent risk related to the vendor. The Due Diligence and High Risk questions/answers, along with the inherent risk, are used to determine the residual risk related to the vendor.

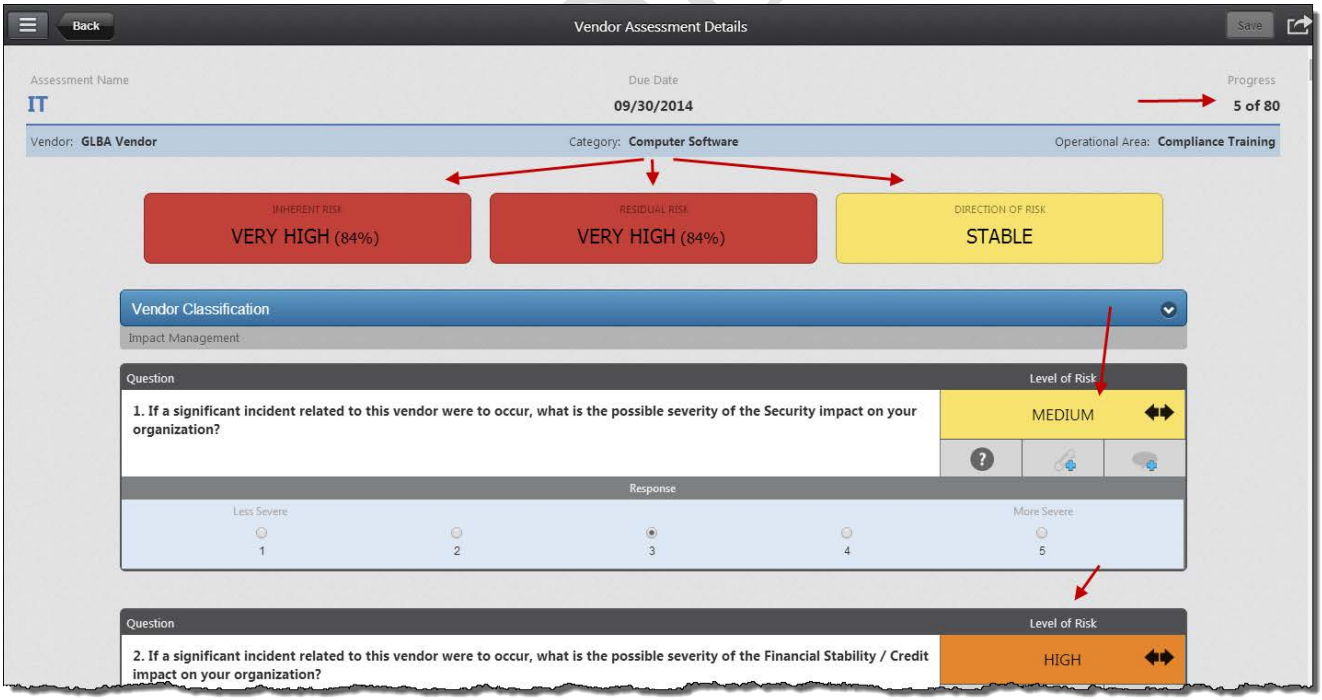
The Direction of Risk shows trends based on previous assessments and assessment questions. For initial assessments, the Direction of Risk will remain Stable as there are no comparison points.

Important Note: In the header of the High Risk section, there is an Opt Out option. If selected, the questions in this section are not required and the entire section is collapsed. The questions will not be considered in calculating the risk values. It is important to note that this is not recommended, particularly for Tier 1 vendors. If the Opt Out is selected, upon finalizing the assessment, an explanation for opting out will be required.

Questions/Answers

Before finalizing the assessment, all questions must be answered.

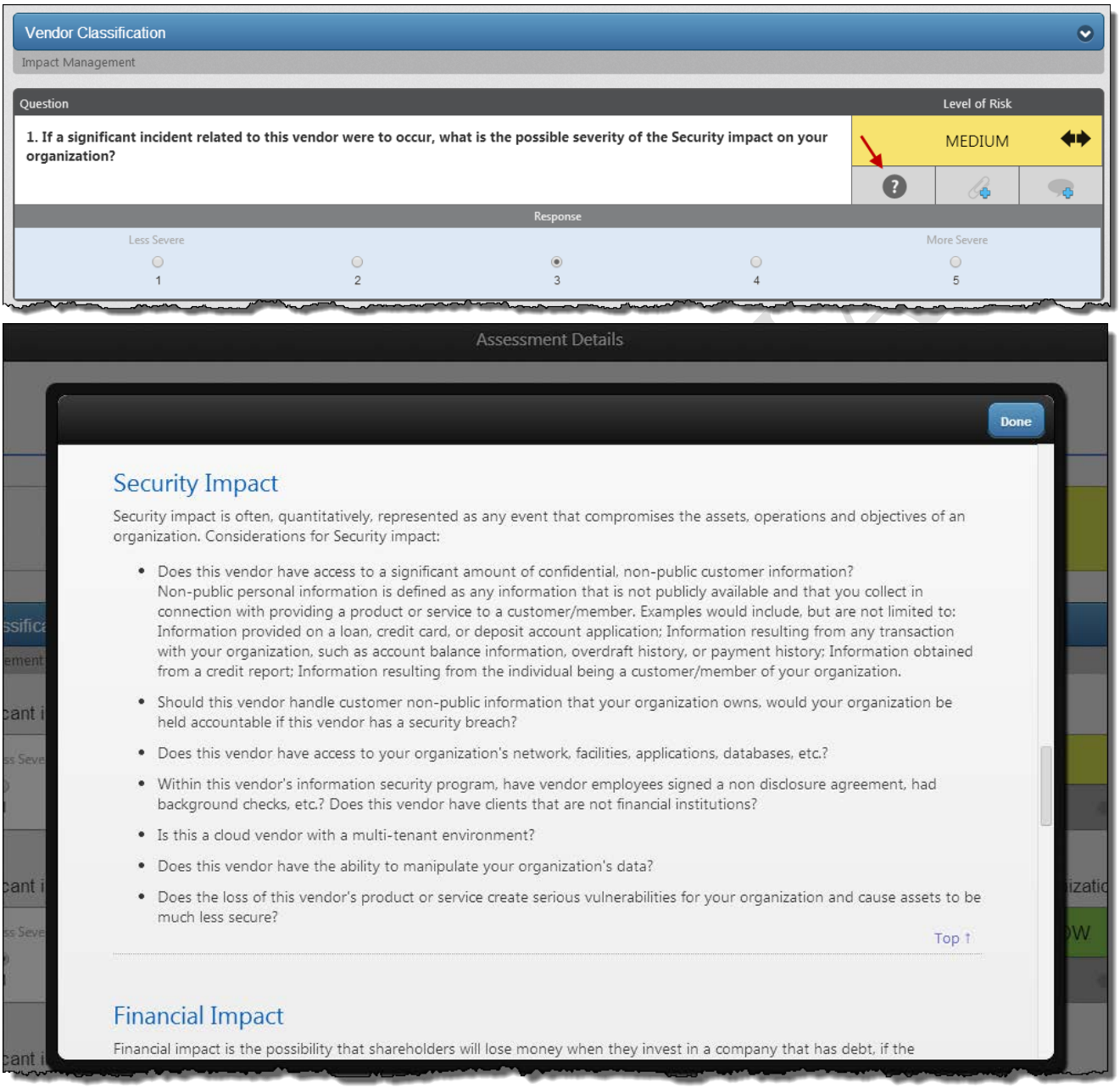
As questions are answered and saved, the risk for each question / answer as well as the overall Inherent Risk, Residual Risk and Direction of Risk are automatically calculated upon saving the assessment. In addition, there is a Progress counter to keep track of how many questions have been answered.



CONFIDENTIAL

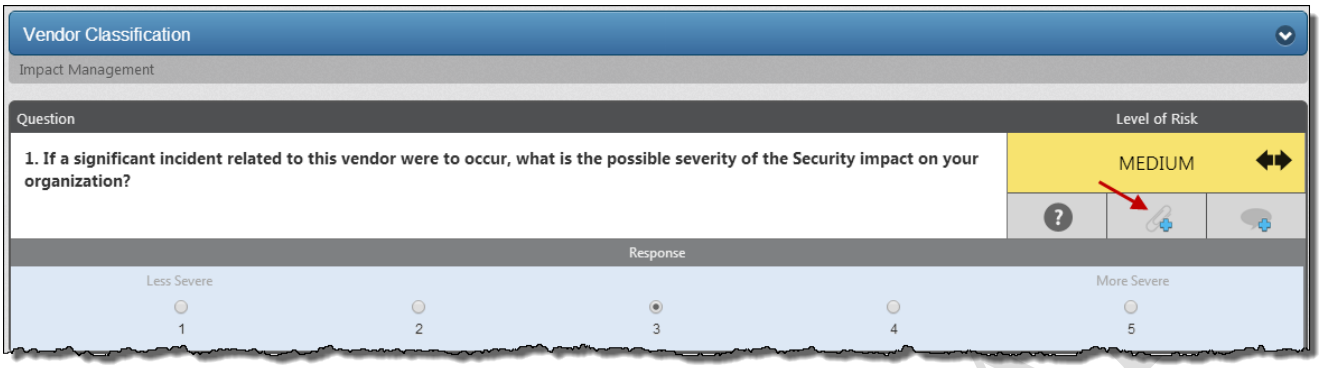
Intelligent Content

Each question has an associated help (?) icon that when selected displays content that describes the purpose of the question.


Vendor Classification
Impact Management
Question
Level of Risk
1. If a significant incident related to this vendor were to occur, what is the possible severity of the Security impact on your organization?
MEDIUM
Response
Less Severe
More Severe
1
2
3
4
5
Assessment Details
Done
Security Impact
Security impact is often, quantitatively, represented as any event that compromises the assets, operations and objectives of an organization. Considerations for Security impact:
Does this vendor have access to a significant amount of confidential, non-public customer information? Non-public personal information is defined as any information that is not publicly available and that you collect in connection with providing a product or service to a customer/member. Examples would include, but are not limited to: Information provided on a loan, credit card, or deposit account application; Information resulting from any transaction with your organization, such as account balance information, overdraft history, or payment history; Information obtained from a credit report; Information resulting from the individual being a customer/member of your organization.
Should this vendor handle customer non-public information that your organization owns, would your organization be held accountable if this vendor has a security breach?
Does this vendor have access to your organization's network, facilities, applications, databases, etc.?
Within this vendor's information security program, have vendor employees signed a non disclosure agreement, had background checks, etc.? Does this vendor have clients that are not financial institutions?
Is this a cloud vendor with a multi-tenant environment?
Does this vendor have the ability to manipulate your organization's data?
Does the loss of this vendor's product or service create serious vulnerabilities for your organization and cause assets to be much less secure?
Top ↑
Financial Impact
Financial impact is the possibility that shareholders will lose money when they invest in a company that has debt, if the

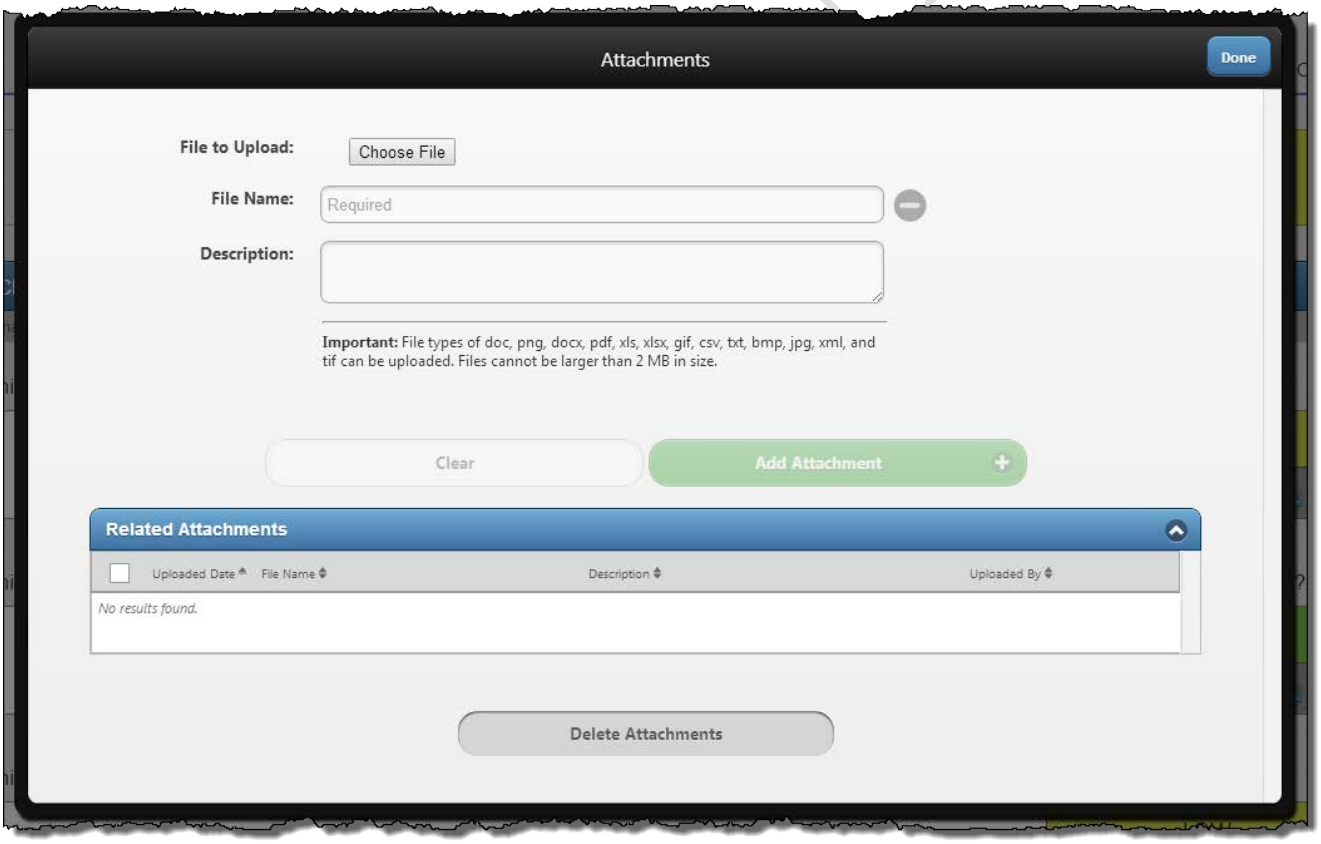
Uploading Attachments to questions

With each question is an option to attach a document(s). Each file cannot be larger than 10MB in size.



Steps to upload an Attachment

1. Select the **attachment icon**. The Attachments page will display in a separate window.

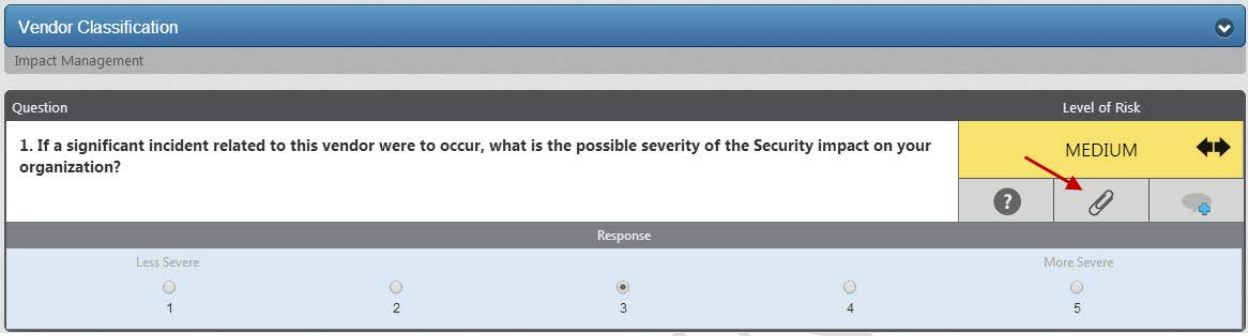


2. Click on the **Choose File** button to browse and select the file to upload.

   Important Note: The list of acceptable file formats to upload is listed under the Description field.

3. The File Name field will automatically populate with the file name of the file being uploaded. If applicable, the file name can be changed.
4. Optionally, provide a description.
5. Select the **Add Attachment** button. The file will be uploaded and placed in the Related Attachments grid. Select the **Done** button (located in the top right of the window) to retain the attachments and return to the Assessment Details page.
6. The attachment icon has now changed from a plus sign to a paper clip.

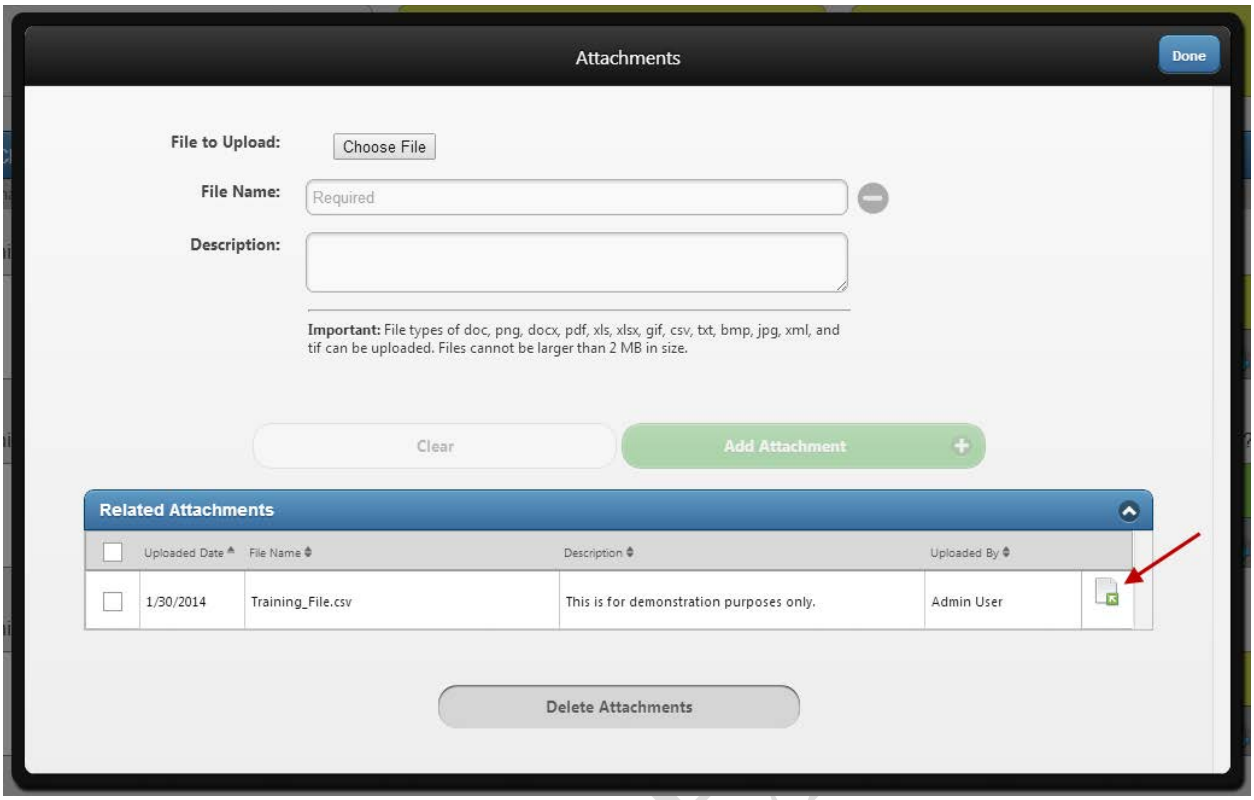
   Important Note: To attach another document to the question, simply select the paper clip icon to launch the Attachments page.



Review the Attachment

1. From the Assessment Details page, select the **paper clip** associated to the question. The Attachments page will display.

CONFIDENTIAL

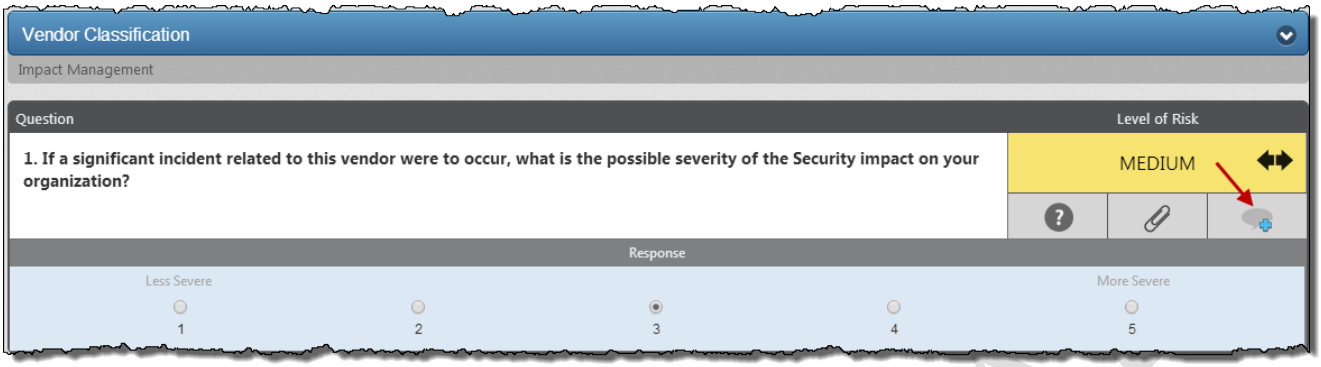


2. Select the icon in the far right row of the attachments. Depending on the file type, the attachment will open in a separate window, or you will be prompted to save the document locally and open.

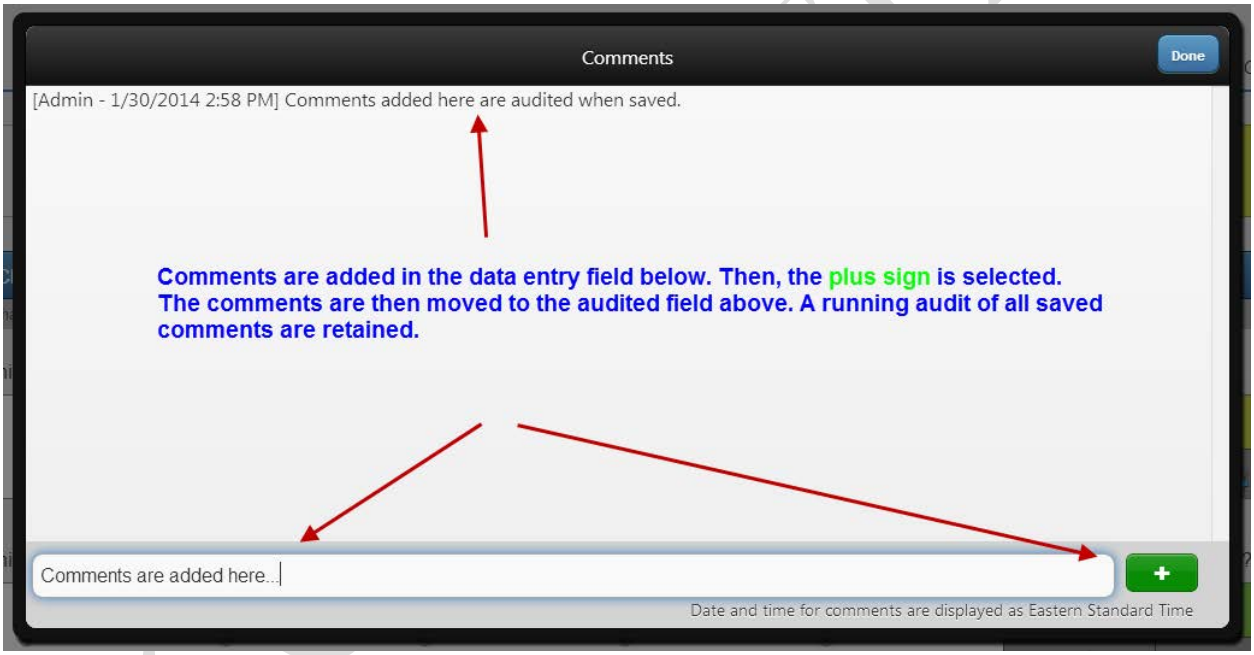
CONFIDE

Assessment Question Comments

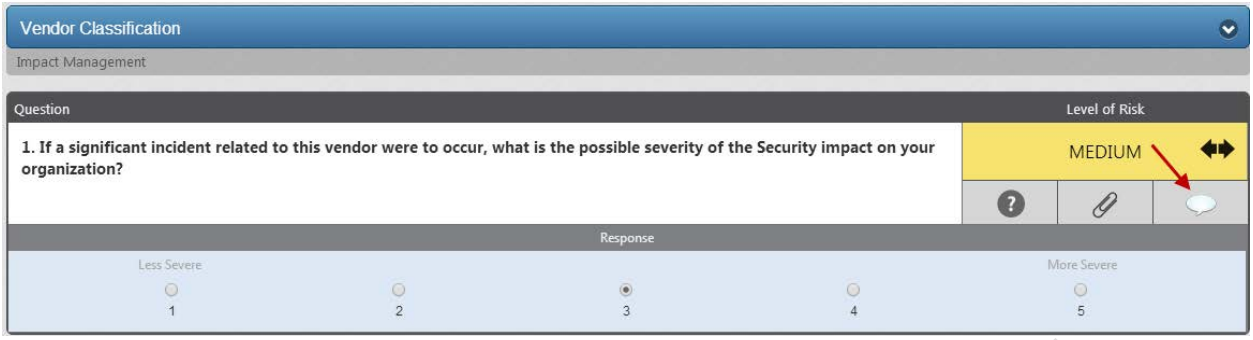
With each question is an option to record audited comments related to the question/answer.



1. Select the **add comments icon**. The Comments page will display.


Comments
Done
[Admin - 1/30/2014 2:58 PM] Comments added here are audited when saved.
Comments are added in the data entry field below. Then, the plus sign is selected. The comments are then moved to the audited field above. A running audit of all saved comments are retained.
Comments are added here...
Date and time for comments are displayed as Eastern Standard Time

2. Enter the comments in the data entry field (to the left of the plus sign). This field accepts up to 1000 alphanumeric characters.
3. Then, select the plus sign. The comments will be moved to the audit field above.
4. Select the **Done** button to return to the Assessment Details page.
5. The grayed out comment bubble and plus sign icons are now replaced with an active comment bubble. Additional comments can be added simply by selecting the comment button to open the Comments page.



Assessment Options Menu

Via the Assessment Details page, there is an Options menu that consists of the following selections:

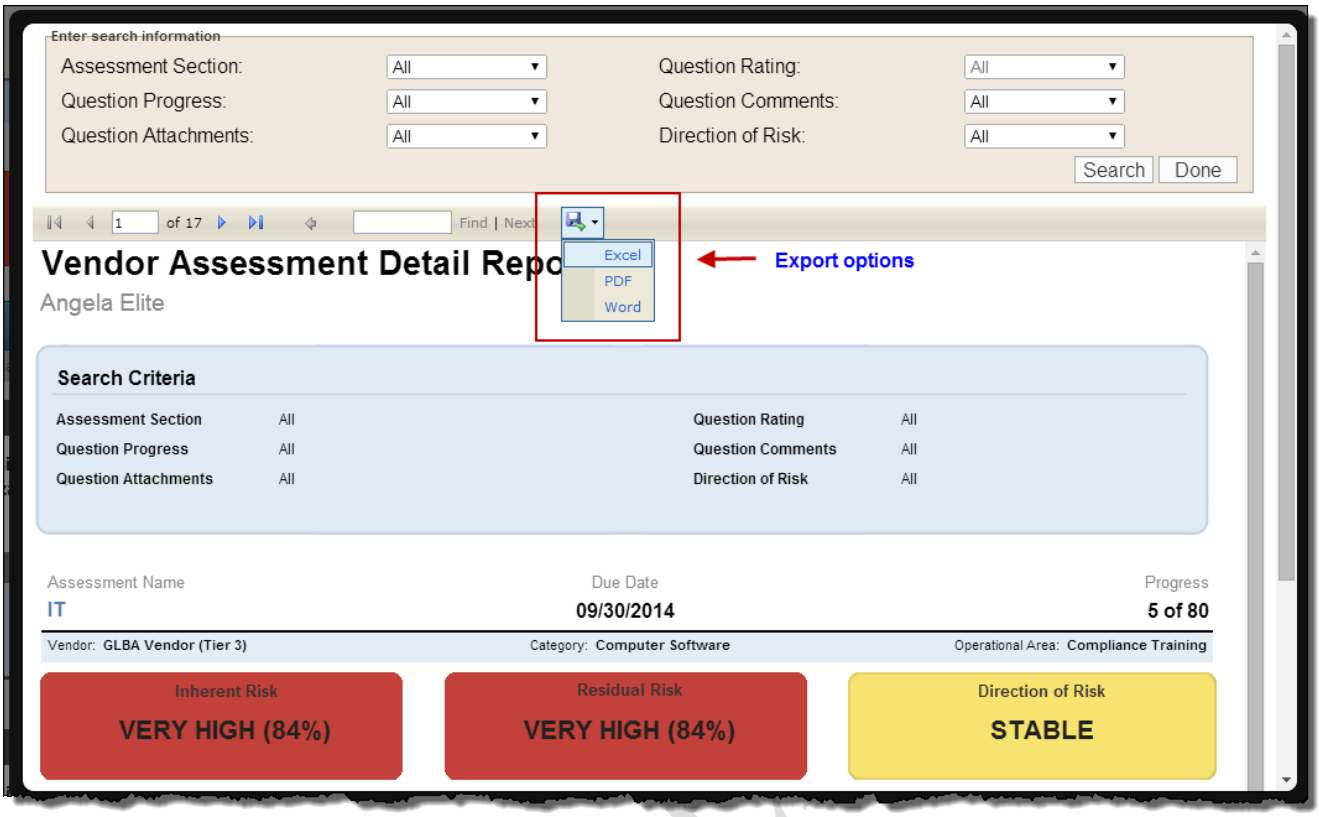
- Vendor Assessment Detail Report
- Edit Assessment Details
- Finalize Assessment – available only after all questions have been answered.

Vendor Assessment Detail Report

To access this report, the user must be associated to a role where the Vendor Assessment Detail Report function is assigned.

1. To run the report, select the **Vendor Assessment Detail Report** option. The report window will display. The search criteria is set by default, but may be optionally changed. After changing, select the Search button to execute the report based on the new query.
2. The report may be exported as a PDF, Microsoft Excel or Word format (see image below).
3. Select the **Done** button to return to the Assessment Details page.

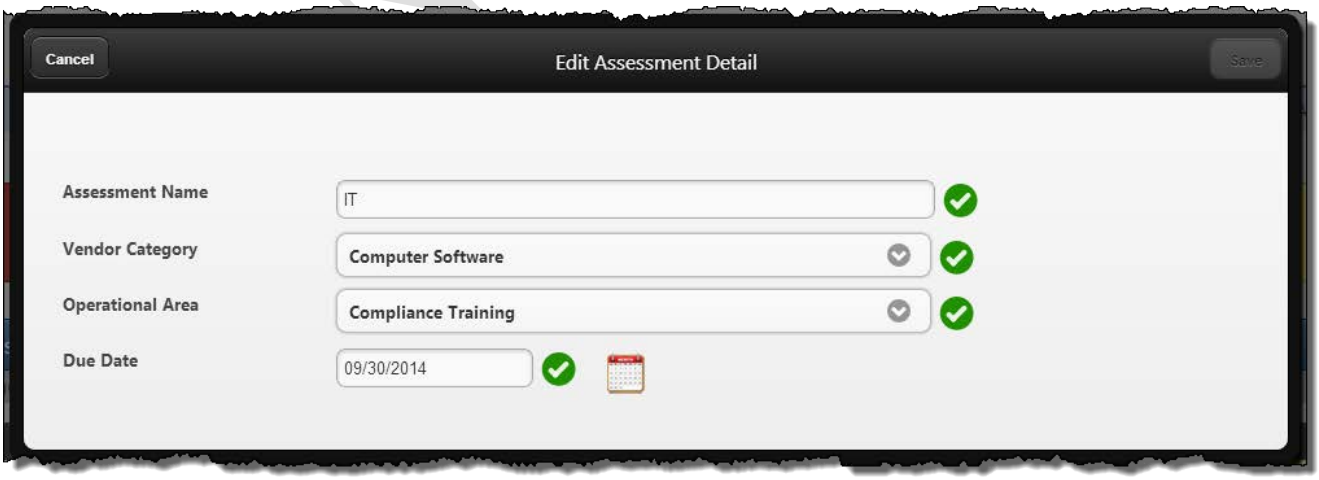
CONFIDENTIAL



Edit Assessment Details

This option will be used in the event the Assessment Name, the category and/or operational area needs to change for a particular assessment.

1. From the Options menu of the Assessment Details, select **Edit Assessment Details**.



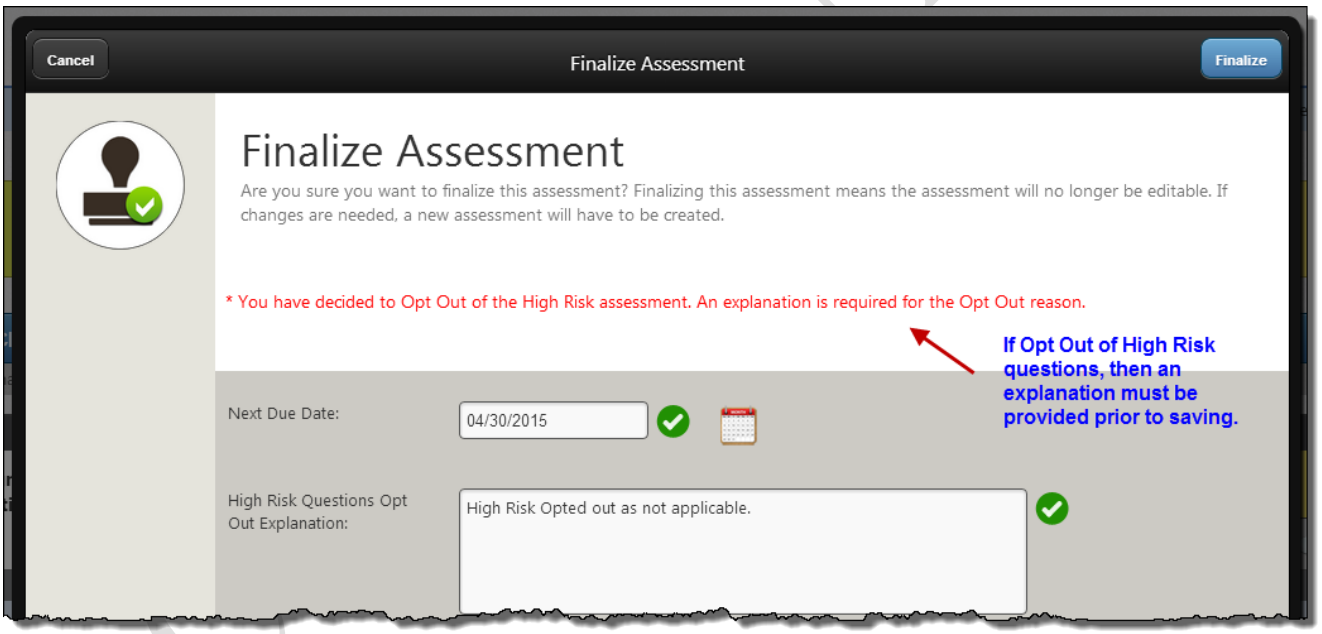
2. Make the applicable changes and then select the **Save** button to return to the Assessment Details page.

3. Upon saving, any changes will be reflected on the Assessment Details page.

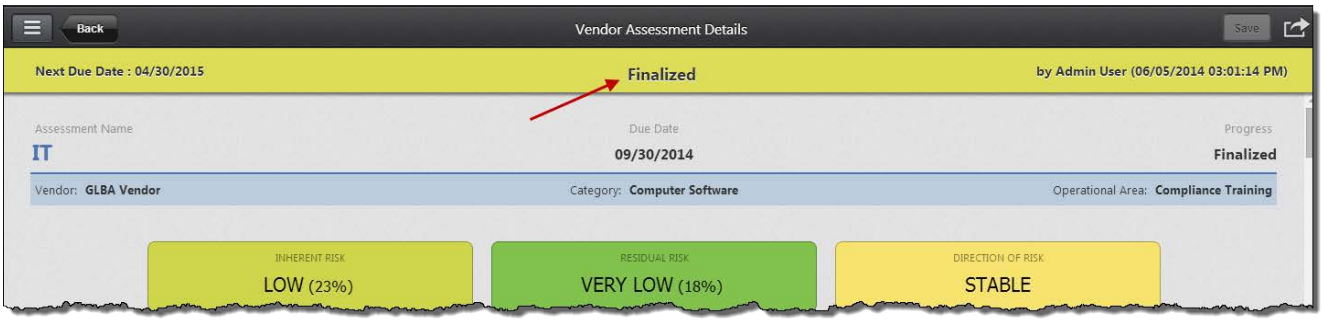
Finalize Assessment

Finalizing the assessment is a way of stating the assessment is now complete. Assessments can be finalized after all questions have been answered.

1. After all questions have been answered and it is time to finalize the assessment, select Finalize Assessment from the Options menu.


Cancel
Finalize Assessment
Finalize
Finalize Assessment
Are you sure you want to finalize this assessment? Finalizing this assessment means the assessment will no longer be editable. If changes are needed, a new assessment will have to be created.
* You have decided to Opt Out of the High Risk assessment. An explanation is required for the Opt Out reason.
If Opt Out of High Risk questions, then an explanation must be provided prior to saving.
Next Due Date:
04/30/2015
High Risk Questions Opt Out Explanation:
High Risk Opted out as not applicable.

2. Prior to completing the process, the **Next Due Date** is required. Simply select the applicable date from the calendar control.
3. Select the **Finalize** button to complete the process.
4. Upon finalizing the assessment, the details page is now read only. No further changes can be made to the assessment. The Vendor Assessment Detail Report is still available in the Options menu.

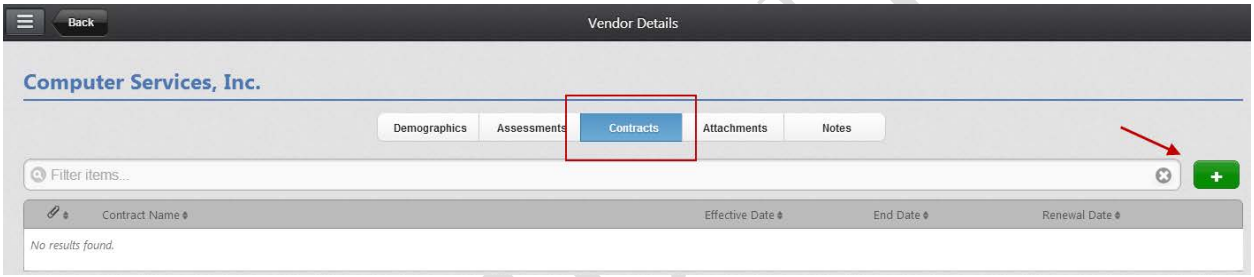


Vendor Contracts

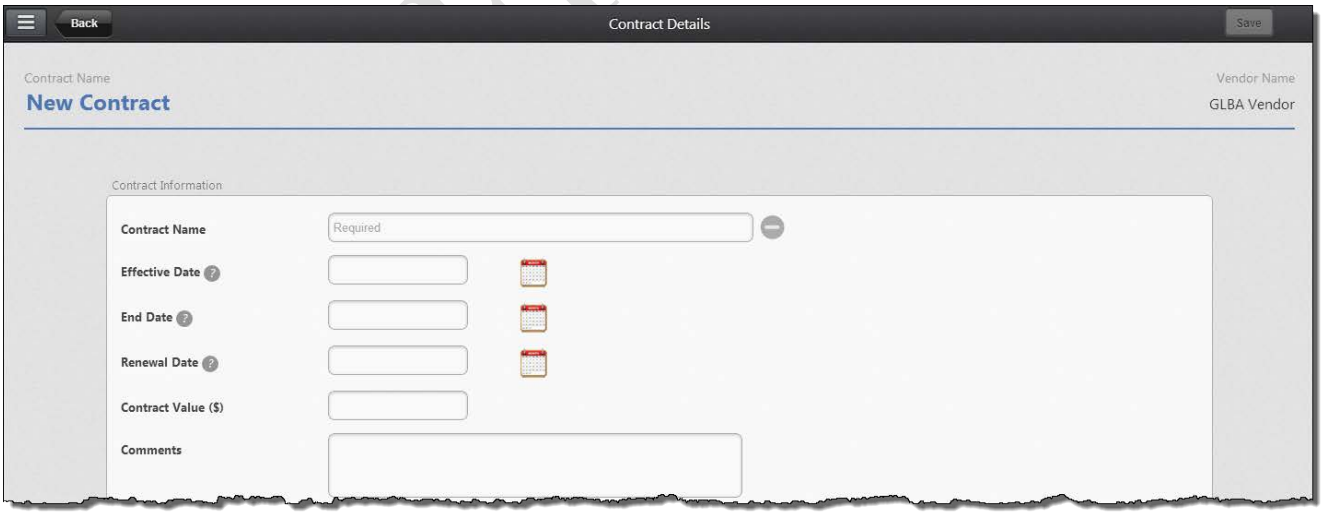
Via the Vendor Details, an entry for each contract associated to the vendor can be created and a copy of the contract can be uploaded for storage.

Steps to create a contract entry

1. From the Vendor Details page of the applicable vendor, select the **Contracts** tab.



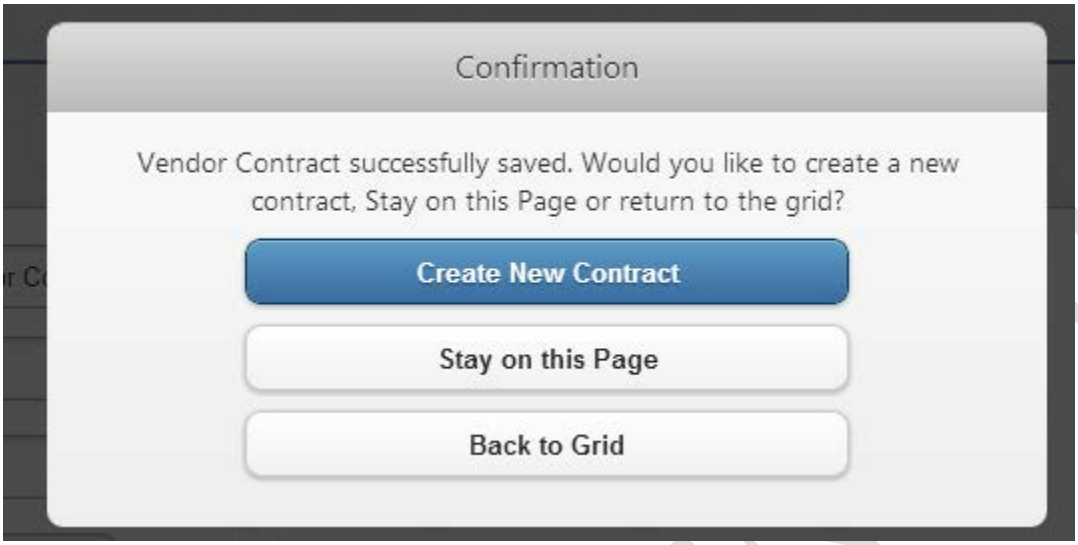
2. Select the plus sign to load the Contract Details page.



3. In the **Contract Name** field, enter a name that contains a maximum of 50 alphanumeric characters.
4. Optionally, use the calendar controls to populate the Effective, End and/or Renewal Date and Contract Value fields.

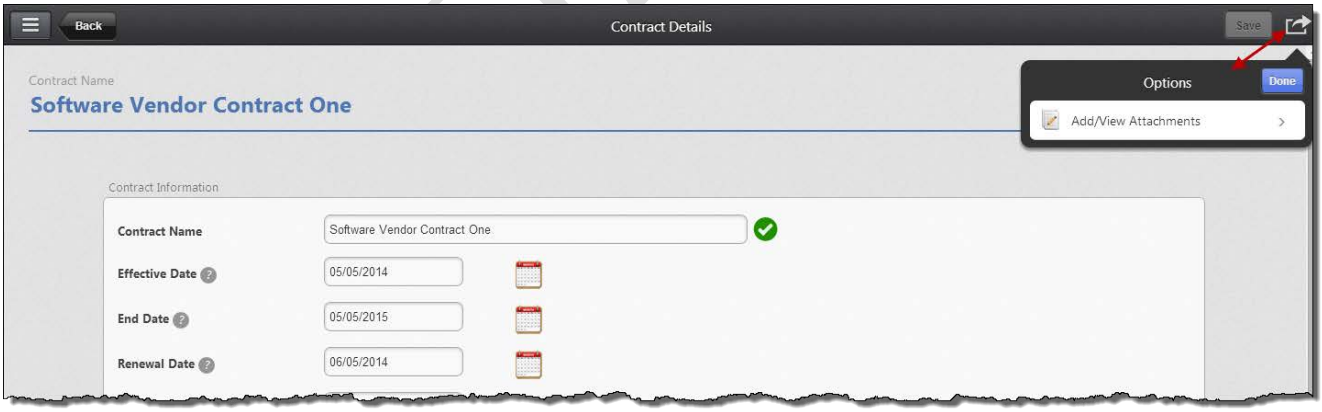
Important Note: Use the help icons associated to the date fields to review the purpose of the dates.

5. Select the **Save** button. The following Confirmation box will be displayed. Please see the following image for the available options.
6. For purposes of training, let's elect to **Stay on this Page**.

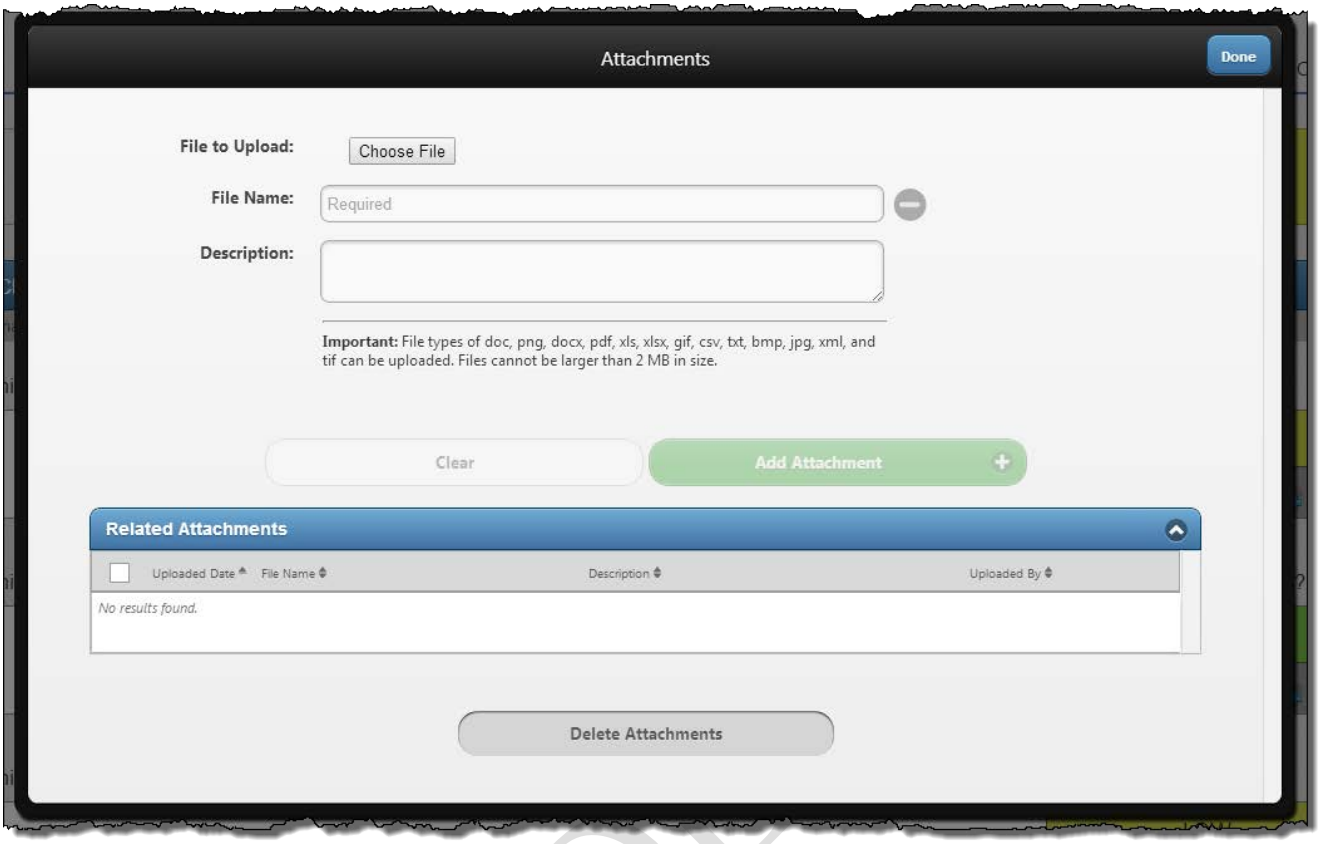

Confirmation
Vendor Contract successfully saved. Would you like to create a new contract, Stay on this Page or return to the grid?
Create New Contract
Stay on this Page
Back to Grid

Steps to upload an Attachment

1. Once the contract has been saved, there is an option to upload attachments to the contract. Select the **Options** menu icon (see following image).



2. Select the **Add/View Attachments** option. The Attachments page will display in a separate window.



3. Click on the **Choose File** button to browse and select the file to upload.

   Important Note: The list of acceptable file formats to upload is listed under the Description field.

4. The File Name field will automatically populate with the file name of the file being uploaded. If applicable, the file name can be changed.

5. Optionally, provide a description.

6. Select the **Add Attachment** button. The file will be uploaded and placed in the Related Attachments grid.

7. Select the **Done** button (located in the top right of the window) to retain the attachments and return to the Contract Details page.

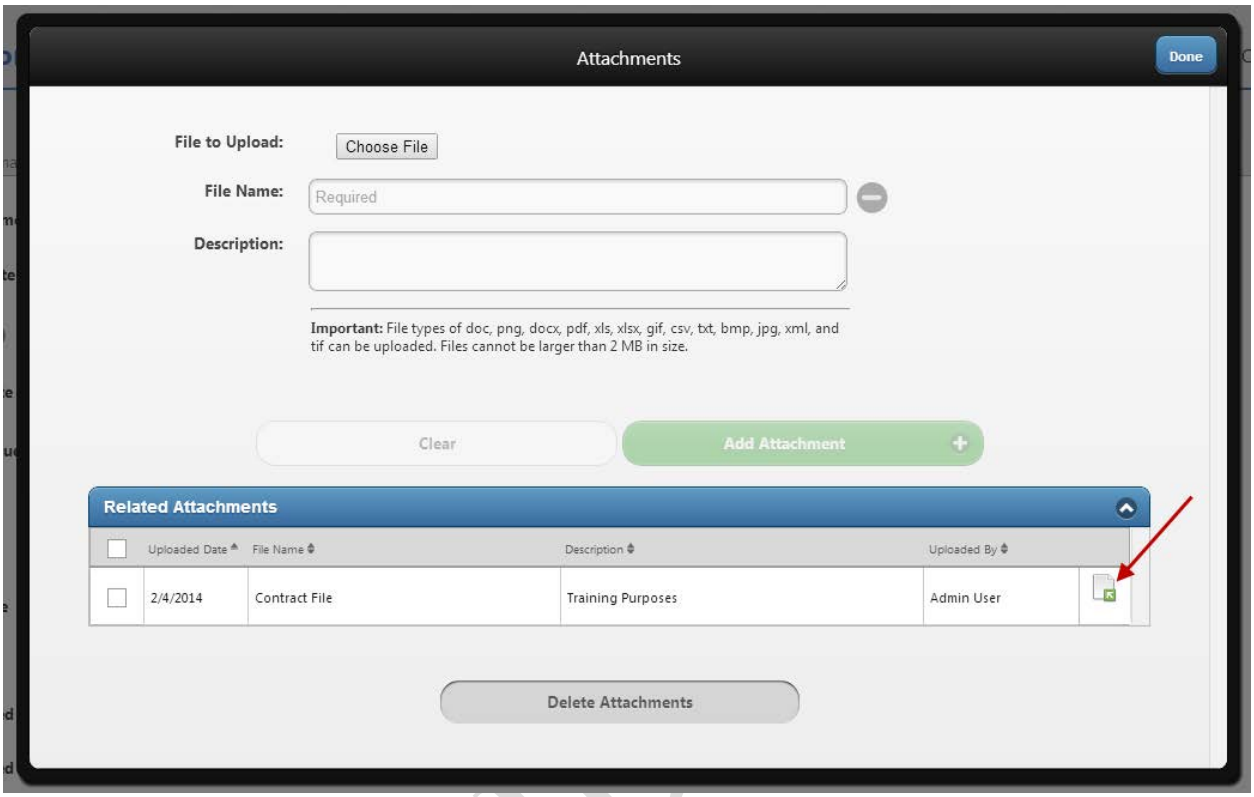
   The attachment icon has now changed from a plus sign to a paper clip.

   Important Note: To attach additional documents to the contract, simply select the paper clip icon or use the Add/View Attachments from the Options menu.

CONFIDE

Review the Contract Attachment

1. From the Contract Details page, select the **paper clip** associated to the question or select Add/View Attachments from the Options menu. The Attachments page will display.

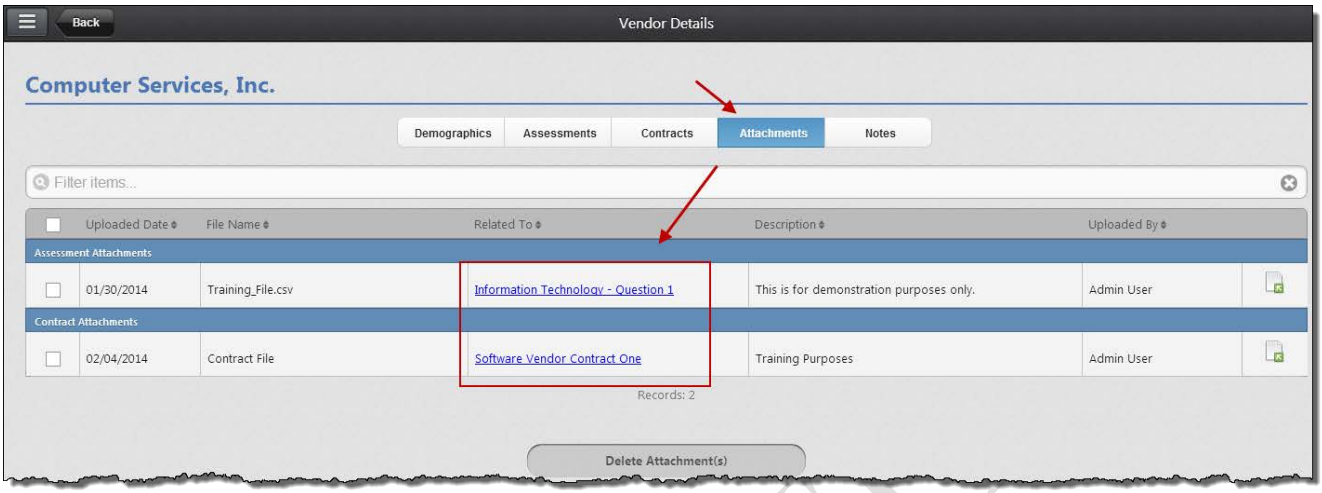


2. Select the icon in the far right row of the attachments. Depending on the file type, the attachment will open in a separate window, or you will be prompted to save the document locally and open.

CONFIDENTIAL

View all Vendor related Attachments

All attachments related to contracts and/or assessment questions that have been uploaded to the site can be found in one repository via the Vendor Details Attachment's tab.

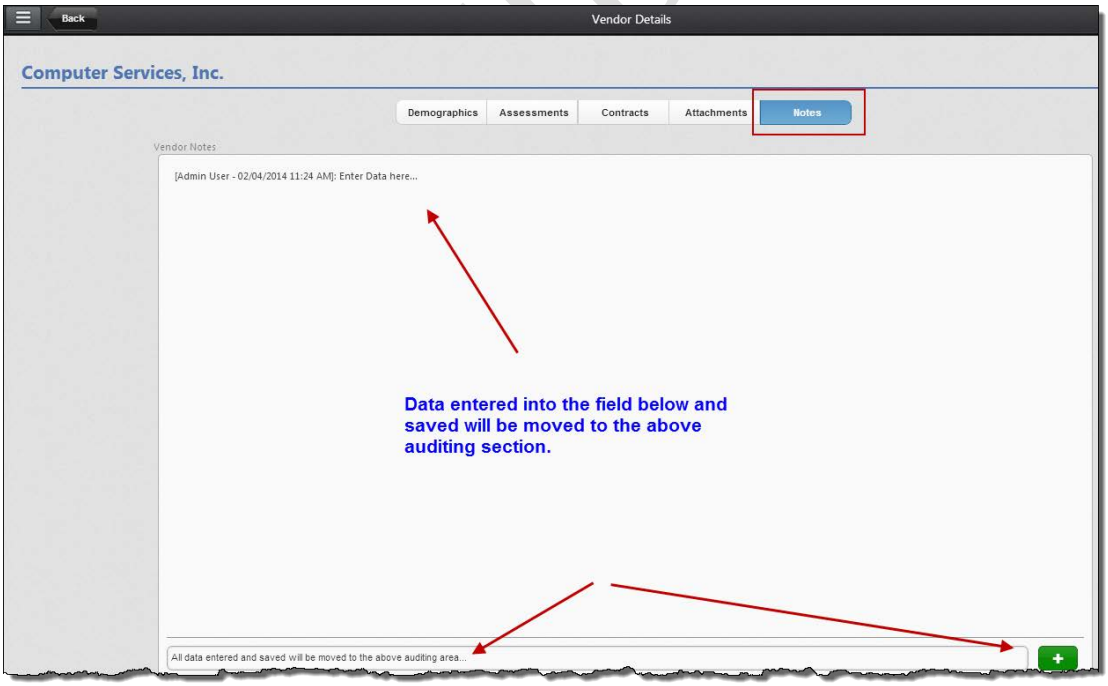


From the Related To column, select the applicable link to be taken directly to either the Contract Details page or the Assessment Details page.

Vendor Notes

From the Vendor Details page, the Notes tab can be used to audit any relevant information about the vendor and its associated parts where there is not an associated field.

1. From the Vendor Details tab, select the **Notes** tab.


Back
Vendor Details
Computer Services, Inc.
Demographics
Assessments
Contracts
Attachments
Notes
Vendor Notes
[Admin User - 02/04/2014 11:24 AM]: Enter Data here...
Data entered into the field below and saved will be moved to the above auditing section.
All data entered and saved will be moved to the above auditing area...

2. Enter any data in the entry field and select the plus sign to save and move the data to the audited section above.

Vendor Reports

From the Options menu on the Vendors page, there are several reports available based on your access level.

Assessment Audit Report

This report includes historical events such as the creation of assessments, auditing of questions/answers, events to attachments related to assessment questions and when the assessment is finalized.

The report is exportable to CSV or Excel.

Assessment Question Detail Report

This report allows for an export of all details related to all assessments across vendors, including the vendor name, assessment name, question text, current answer, inherent risk, and direction of risk.

This report is exportable to CSV or Excel.

Assessment Summary Report

This report provides a snapshot of each assessment, its associated category, operational area, vendor tier and risk values as well as the progress of the assessment (based on number of questions answered).

This report is exportable to Excel, PDF or Word.

Contract Audit Report

This report details historical events such as the creation and deletion of contracts, modified effective and end dates, renewal dates as well as modified contract values and events of attachments to the contracts.

This report is exportable to Excel, PDF or Word.

Contract Summary Report

This report provides a snapshot of the contract(s) for all vendors, associated effective and end dates as well as the renewal date, the number of attachments and the current status of the vendor.

This report is exportable to Excel, PDF or Word.

Demographic Audit Report

This report provides a detailed history of the changes made to several fields from the demographics page such as tier assignments as well as category and operational area assignments.

This report is exportable to Excel, PDF or Word.

Demographic Summary Report

This report provides a snapshot of the vendor demographics, its associated owner, category, and operational area.

This report is exportable to Excel, PDF or Word.

CONFIDENTIAL

Vendor Summary Report

This summary report provides a comprehensive overview of each Vendor. The report includes vendor tier, vendor name, contract amount, contract effective, end, and renewal dates, vendor data access levels, and risk assessment activity. The report can be filtered by vendor, operational area, tier, risk level, or vendor owner.

This report is exportable to Excel, PDF or Word.

Vendor Batch Screening Report (Export)

This report enables users to generate a CSV file containing all their vendors so that information can then be uploaded into the Watch List Screening module of WatchDOG Elite for batch sanction screening. This report includes a system generated Vendor ID, Vendor Name, Street Address, City, State, Postal Code, and Country.

This report is exportable to CSV.

Vendor Batch Screening Contacts Report (Export)

This report enable users to generate a CSV file containing all their vendor contacts so that information can then be uploaded into the Watch List Screening module of WatchDOG Elite for batch sanction screening. This report includes Vendor Name, a system generated Contact ID, Contact Name, Street Address, City, State, Postal Code, and Country.

This report is exportable to CSV.

This completes the Vendor Management section.

CONFIDENTIAL

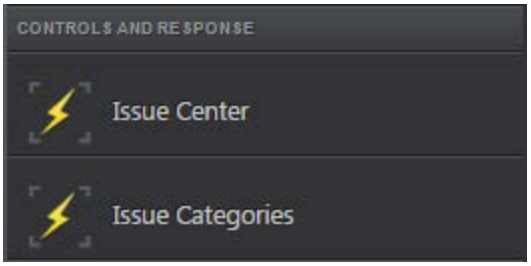
Controls and Response Overview

The Controls and Response module in WatchDOG Elite will enable users to log and track a wide variety of findings, matters, issues, and tasks related to Regulatory Compliance activities as part of the control, remediation and response process.

This section currently contains the Issue Center and Issue Categories links.

Navigation:

The Controls and Response section will be displayed within the left side Navigation toolbar as:



Only those links which the user has access to via security functions will be available in the Navigation toolbar.

Following is an explanation of the links within this section.

Controls and Response Introduction – Issue Center Features and Functions

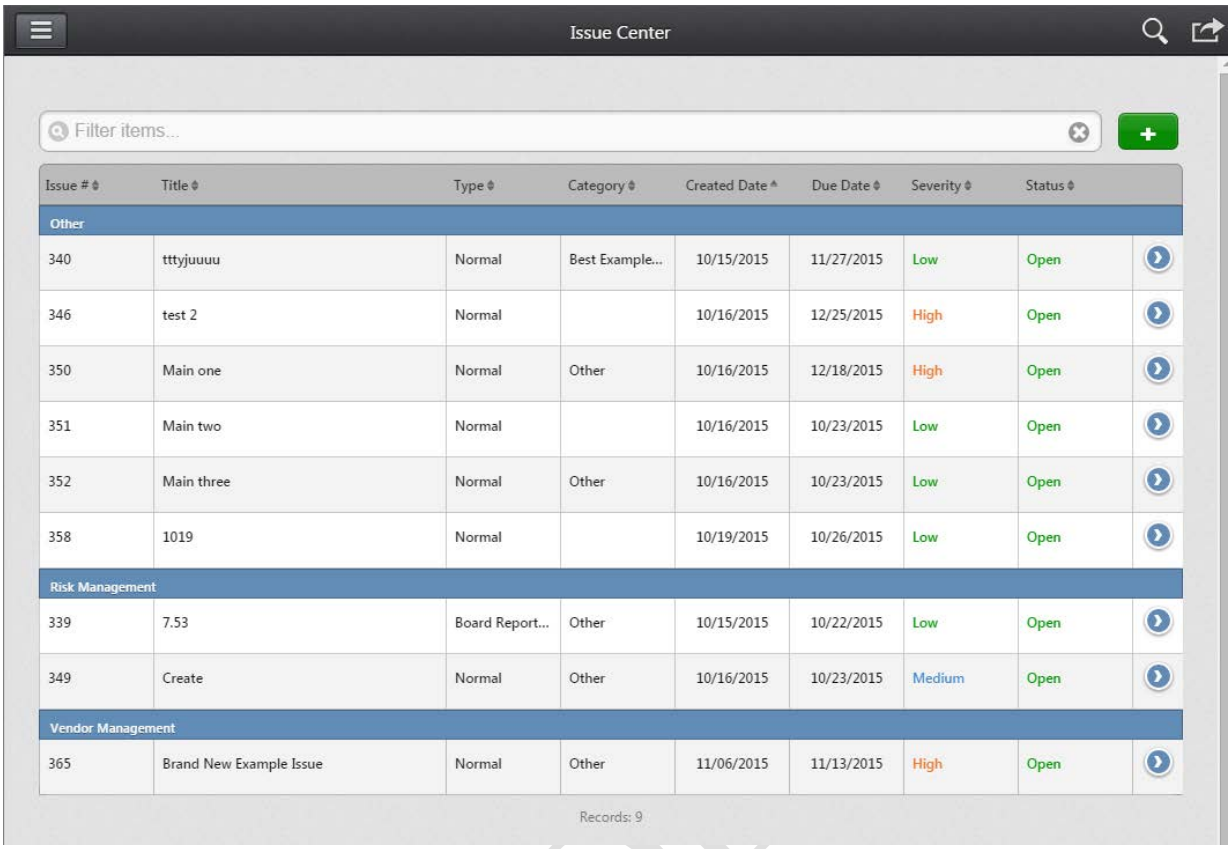
Issue Center can provide support in keeping track of assessment, audit, and exam findings as well as tasks that arise throughout the normal course of business.

Refer to the full Admin User Manual to review all Administrative and User Functions for this module.

Viewing and Navigating the Issue Center Page

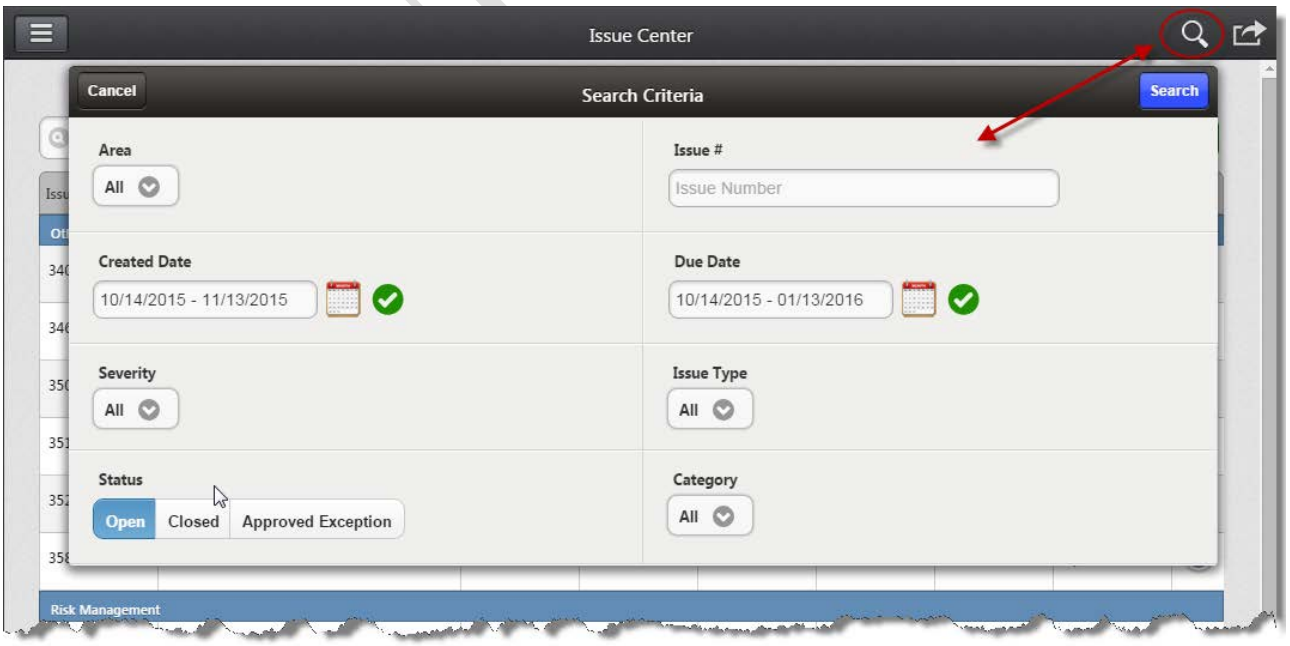
1. Select the **Issue Center** link. The Issue Center grid will display. All issues have a unique issue number and are grouped by area.

CONFIDENTIAL

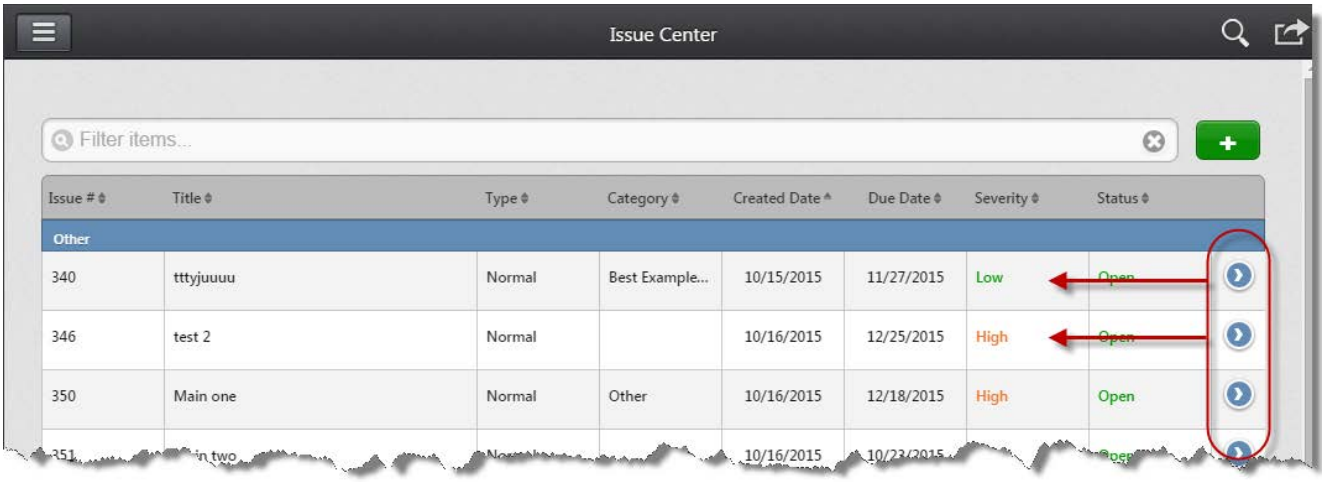

Issue Center
Filter items...
Issue # | Title | Type | Category | Created Date | Due Date | Severity | Status
Other
340 | tttyjuuuu | Normal | Best Example... | 10/15/2015 | 11/27/2015 | Low | Open
346 | test 2 | Normal | | 10/16/2015 | 12/25/2015 | High | Open
350 | Main one | Normal | Other | 10/16/2015 | 12/18/2015 | High | Open
351 | Main two | Normal | | 10/16/2015 | 10/23/2015 | Low | Open
352 | Main three | Normal | Other | 10/16/2015 | 10/23/2015 | Low | Open
358 | 1019 | Normal | | 10/19/2015 | 10/26/2015 | Low | Open
Risk Management
339 | 7.53 | Board Report... | Other | 10/15/2015 | 10/22/2015 | Low | Open
349 | Create | Normal | Other | 10/16/2015 | 10/23/2015 | Medium | Open
Vendor Management
365 | Brand New Example Issue | Normal | Other | 11/06/2015 | 11/13/2015 | High | Open
Records: 9

Note: Users with the Issue View function will only be able to view issues that are assigned to them. Users with the Issue Create function will be able to view issues that they have created as well as issues that are assigned to them. Users with the Issue Maintenance function will be able to view all issues regardless of assignment or creation.

2. To perform a search of the grid, select the search icon. The Search Criteria box will display.



3. Set the applicable search criteria and select the **Search** Button. Results based on the criteria will be displayed in the Issue Center grid.
4. You may also use the Inline Search Filter to search the grid for a particular issue(s).
5. To view a particular issue on the Issue Center grid, select the blue arrow or click the row associated to the item to be viewed.


Issue Center
Filter items...
Issue # Title Type Category Created Date Due Date Severity Status
Other
340 tttyjuuuu Normal Best Example... 10/15/2015 11/27/2015 Low Open
346 test 2 Normal 10/16/2015 12/25/2015 High Open
350 Main one Normal Other 10/16/2015 12/18/2015 High Open

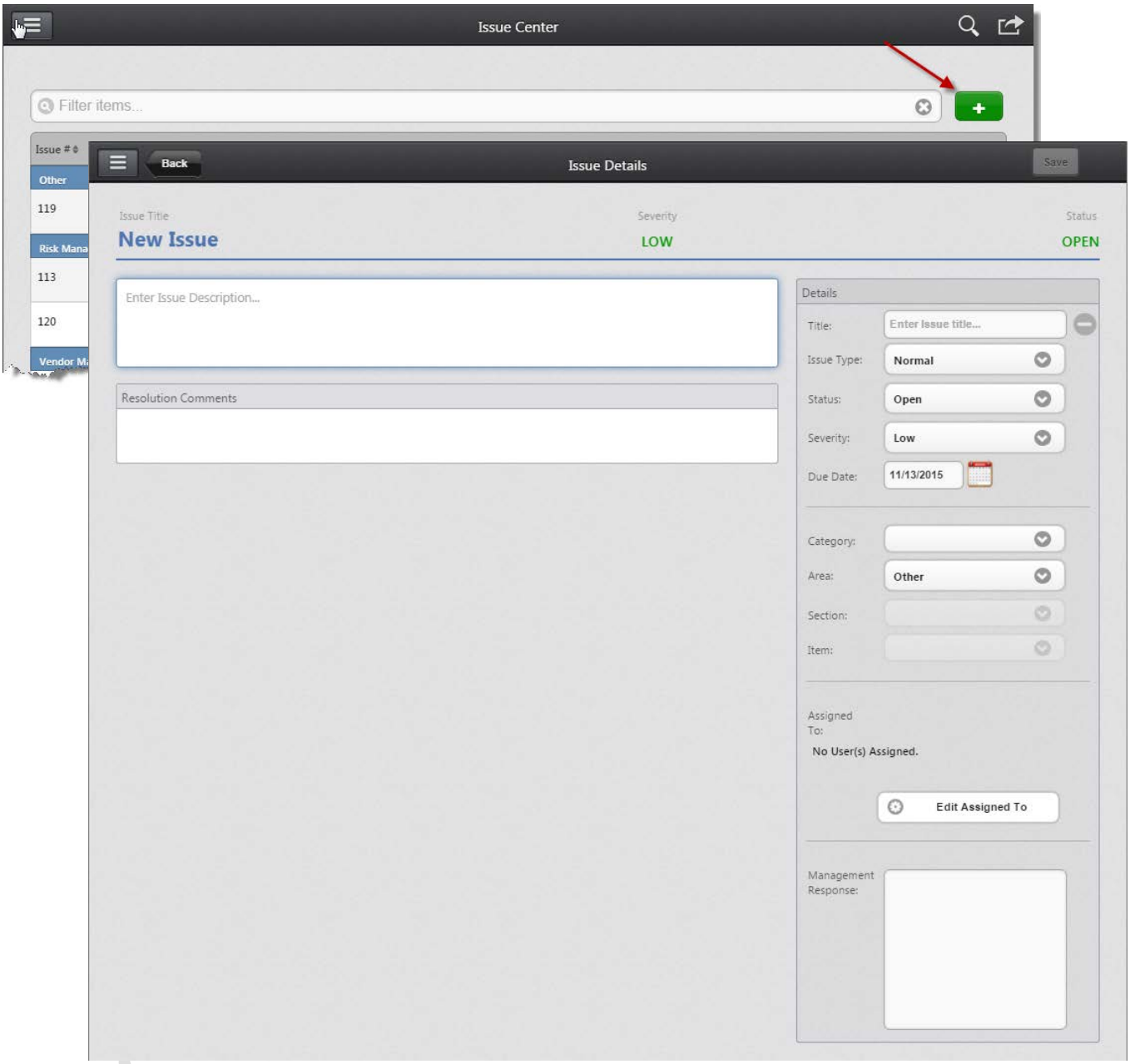
6. The Issue Details page will be displayed.

Issue Center – Create and Manage a New Issue

Create a New Issue

1. Select the **Issue Center** link. The Issue Center grid will display.
2. To create an issue, select the green plus sign. The Issue Details page will display.

CONFIDEN

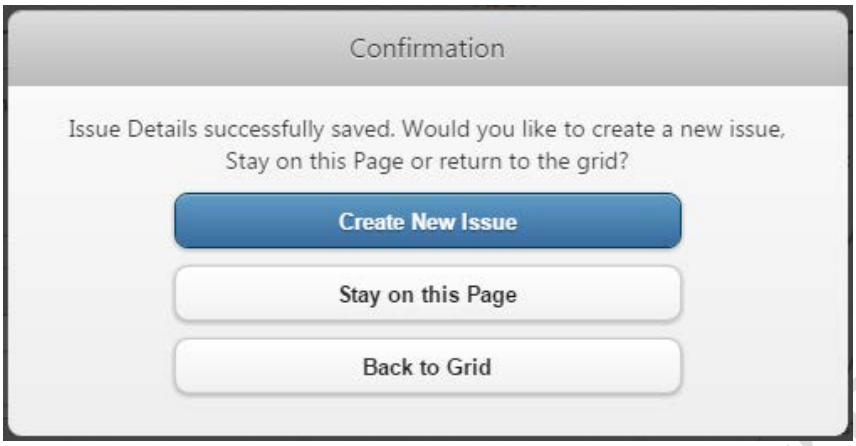


3. In the required **Title** field, provide a title that contains a maximum of 100 alphanumeric characters.
4. Optionally, provide an **Issue Description** that contains no more than 1000 alphanumeric characters.
5. Select the applicable choices for the **Issue Type**, **Status**, **Severity**, **Due Date**, **Category**, **Area**, **Section**, and **Item** fields if their values differ from the default values given.

   Note: For a user with the Issue Maintenance function, the Status dropdown will have an additional choice called *'Approved Exception'*.

   The **Area** field defaults to 'Other'. The selections on this dropdown depend on the product areas that the client has access to in the WatchDOG Elite application. The **Section** and **Item** values will depend on the Area selected from the dropdown.

6. Optionally, add up to 10 users to the new issue by selecting the **Edit Assigned To** button in the Assigned To section of the Details.
7. Once all selections have been made, select the **Save** button at the top of the page. A confirmation message box will appear:


Confirmation
Issue Details successfully saved. Would you like to create a new issue, Stay on this Page or return to the grid?
Create New Issue
Stay on this Page
Back to Grid

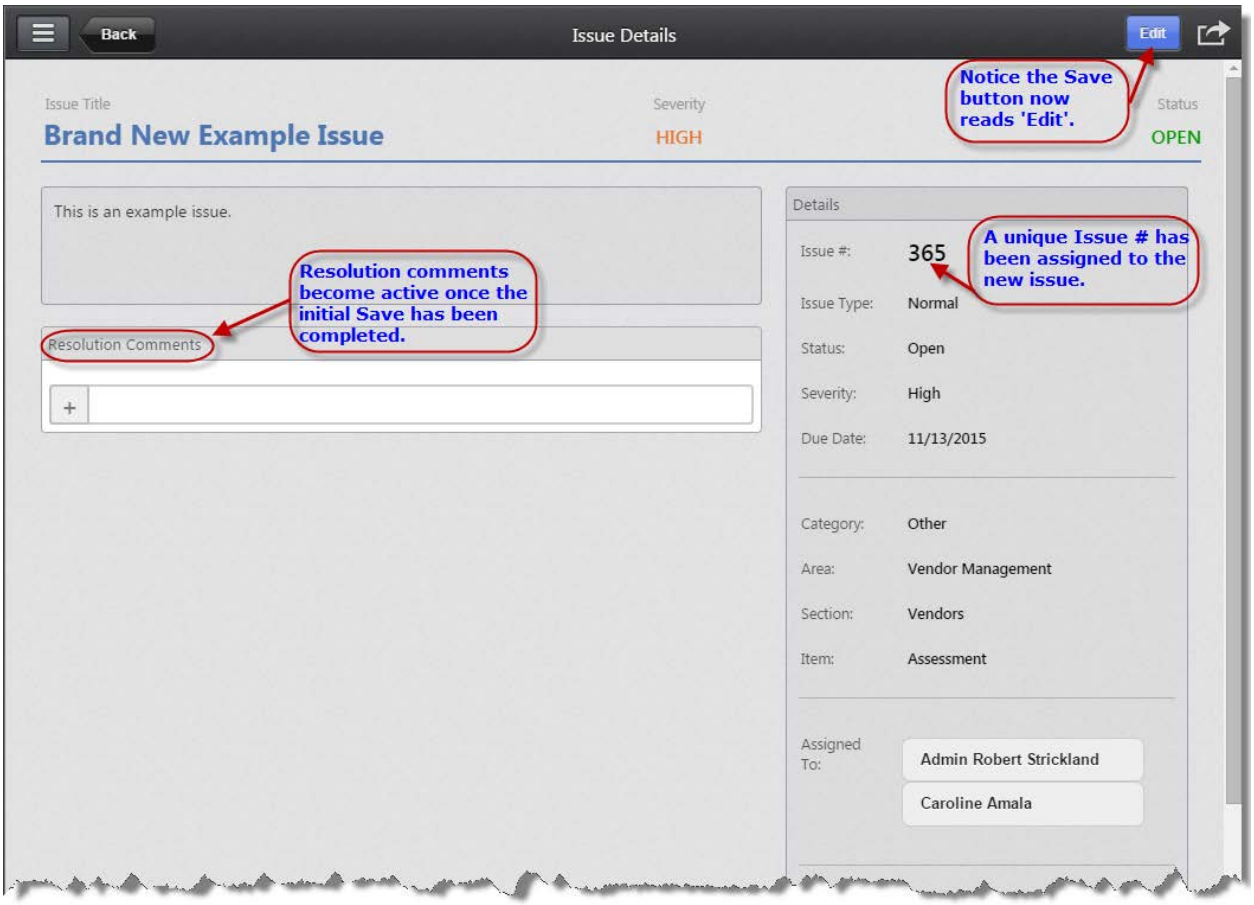
- Clicking *'Create New Issue'* will present a blank Issue Details page with default values and give the user the ability to create a new issue.
- Clicking *'Stay on this Page'* will allow the user to remain on the current page with the newly created issue.
- Clicking *'Back to Grid'* will direct the user back to the Issue Center page to view the newly created issue in its respective area on the grid.

Note: Once the issue has been successfully saved, the Save button will now read 'Edit'. Also, if there are any users assigned to the issue, a notification email will be sent out to the assignees.

Issue Assignment Notification
watchdognotifications@csiweb.com
Sent: Mon 10/12/2015 10:59 AM
To:
You have been assigned the following issue:
Issue#: 126
Title: Brand New Example Issue
Description: This is an example issue description that I am entering to show all users how this can be done.
Issue Type: Normal
Due Date: 10/23/2015
Please log in to WatchDOG Elite to view the issue.
Thanks,
System Support

To complete this issue creation, we will select to 'Stay on this Page'.

CONFIDENTIAL



8. Since the initial save was completed, the **Resolution Comments** section is active and comments can be added to the new issue. Refer to the *'Issue Details – Managing Resolution Comments'* section in the Admin User Manual for more details.
9. Optionally, add attachments to the new issue via the Options menu on the Issue Details page. Refer to the *'Issue Details – Add/View Attachments'* section in the Admin User Manual for more details.

Editing an Issue

Refer to the full Admin User Manual for a complete list of editable fields per function.

Steps to Edit an Issue

1. Select the **Edit** button at the top of the Issue Details page. Depending on the users function assignment, fields will open for editing. The Edit button now reverts back to read 'Save'.

2. Once all updates to the issue have been made, select the **Save** button to accept the changes. A message will appear: *"This issue was saved successfully."*

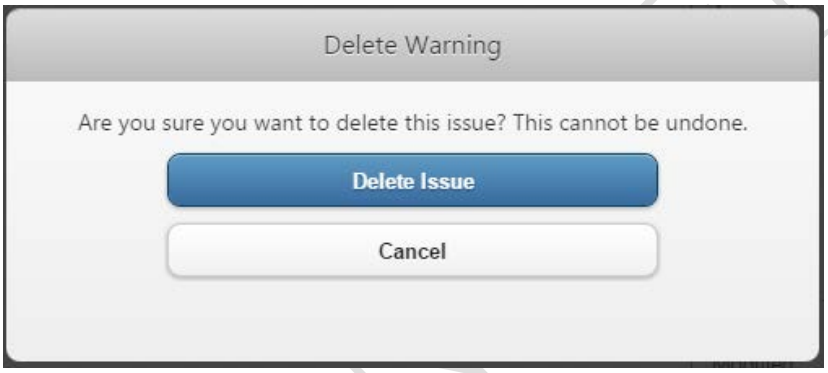
CONFIDENTIAL

Issue Details – Deleting an Issue

Steps to Delete an Issue

1. Select the issue to be deleted from the Issue Center page. The Issue Details page for that issue will be opened.
2. Scroll down to the bottom of the page below the Attachments grid to view the Delete Issue button.

3. Select the **Delete Issue** button at the bottom of the page. A Delete Warning message will pop up, *"Are you sure you want to delete this issue? This cannot be undone."*

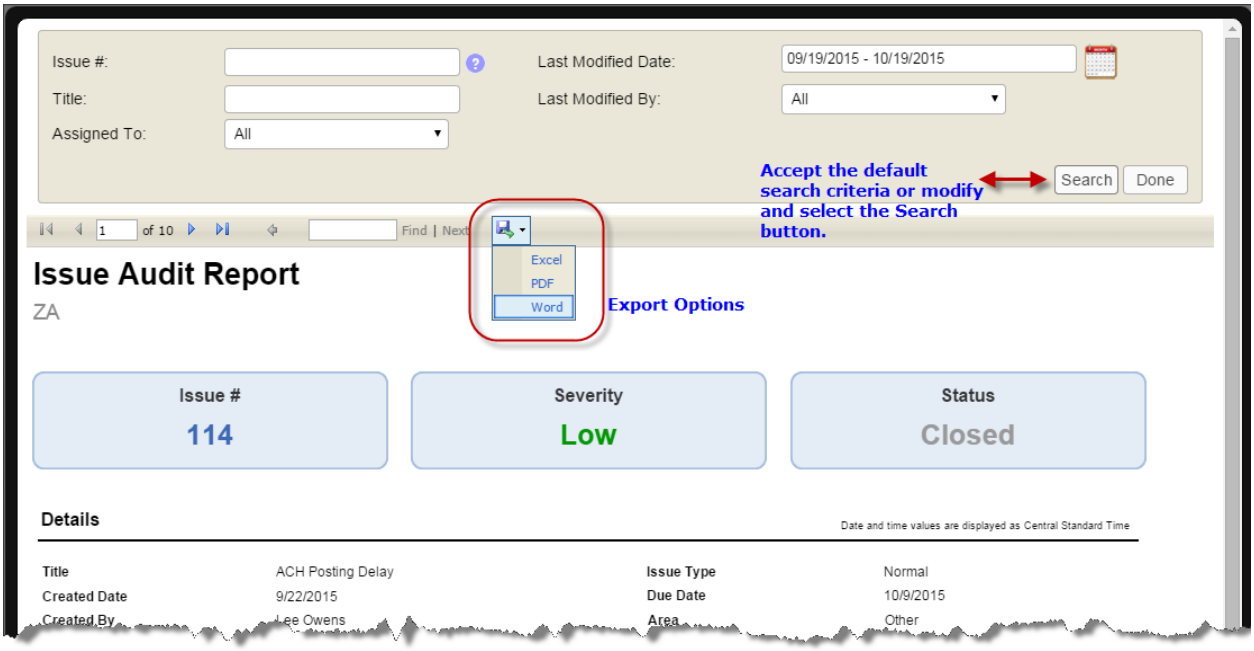


- Clicking *'Delete Issue'* will immediately delete the issue and direct the user back to the Issue Center grid.
- Clicking *'Cancel'* will close the message box and return the user to the Issue Details page.

Issue Center Reports

From the Options menu on both the Issue Center page and the Issue Details page, there are reports available based on your assigned functions. Please see Issue Center Administrative and User functions in the full Admin User Manual for an explanation of each report.

1. To run a particular report, simply select the applicable option and access the defaults or change the search settings.



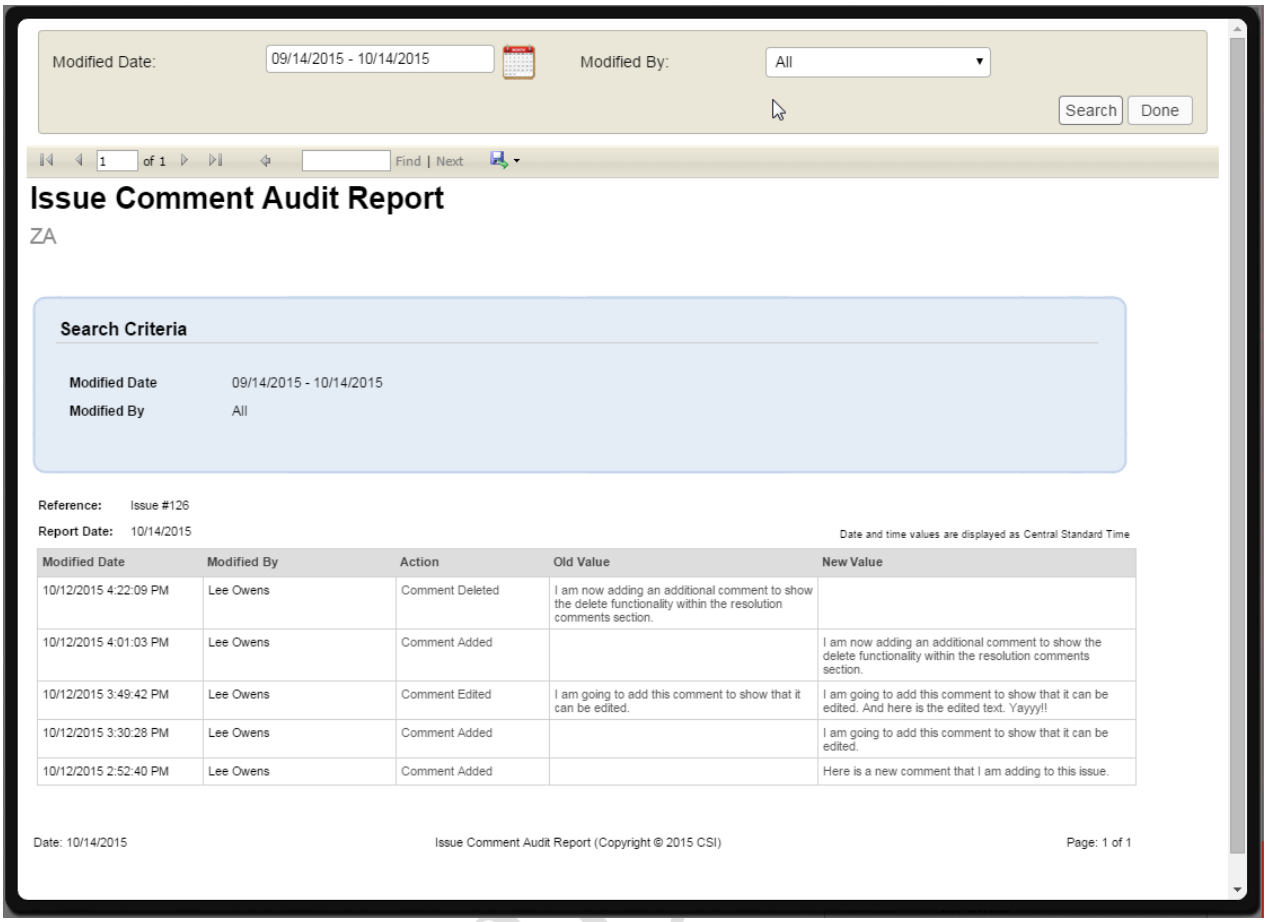
2. Optionally, the results of each report may be exported as a PDF, Microsoft Excel or Word format.

Issue Comment Audit Report

In addition to the function-driven reports referenced above, the Issue Comment Audit Report is available to all users and can be viewed by the assigned users of a particular issue. This report can be accessed via the Options menu on the Issue Details page.

The Issue Comment Audit Report will audit any and all activity within the Resolution Comments section on the Issue Details of an issue. Actions such as when a comment is added, edited, or deleted can be tracked on this report.

CONFIDENTIAL

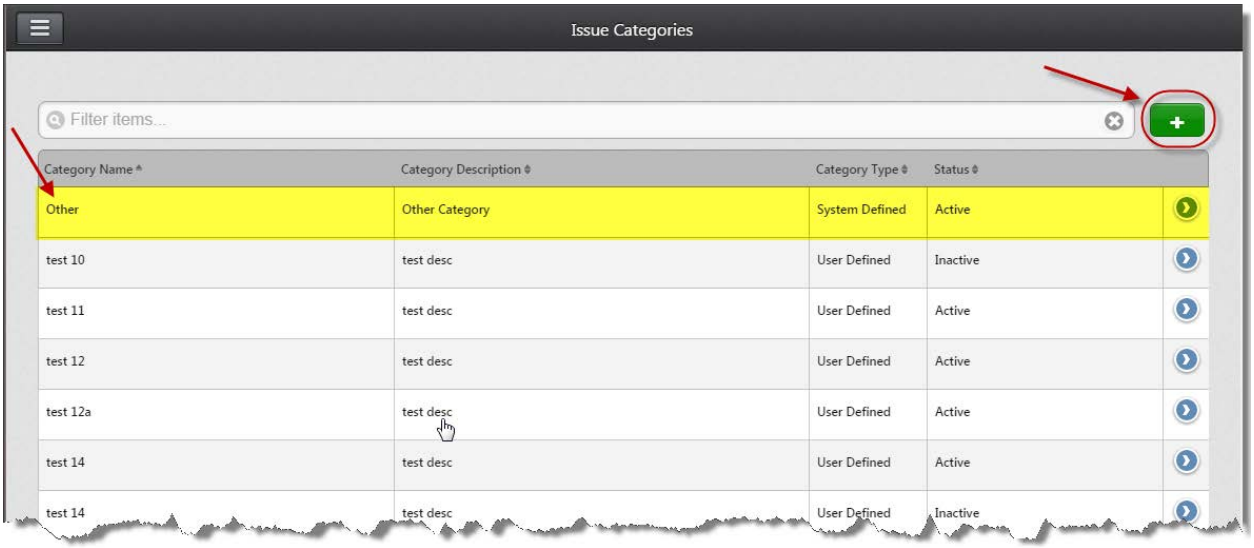

Modified Date:
09/14/2015 - 10/14/2015
Modified By:
All
Search
Done
1
of 1
Find | Next
Issue Comment Audit Report
ZA
Search Criteria
Modified Date
09/14/2015 - 10/14/2015
Modified By
All
Reference:
Issue #126
Report Date:
10/14/2015
Date and time values are displayed as Central Standard Time
Modified Date
Modified By
Action
Old Value
New Value
10/12/2015 4:22:09 PM
Lee Owens
Comment Deleted
I am now adding an additional comment to show the delete functionality within the resolution comments section.
10/12/2015 4:01:03 PM
Lee Owens
Comment Added
I am now adding an additional comment to show the delete functionality within the resolution comments section.
10/12/2015 3:49:42 PM
Lee Owens
Comment Edited
I am going to add this comment to show that it can be edited.
I am going to add this comment to show that it can be edited. And here is the edited text. Yayyy!!
10/12/2015 3:30:28 PM
Lee Owens
Comment Added
I am going to add this comment to show that it can be edited.
10/12/2015 2:52:40 PM
Lee Owens
Comment Added
Here is a new comment that I am adding to this issue.
Date: 10/14/2015
Issue Comment Audit Report (Copyright © 2015 CSI)
Page: 1 of 1

Issue Categories – Create and Manage

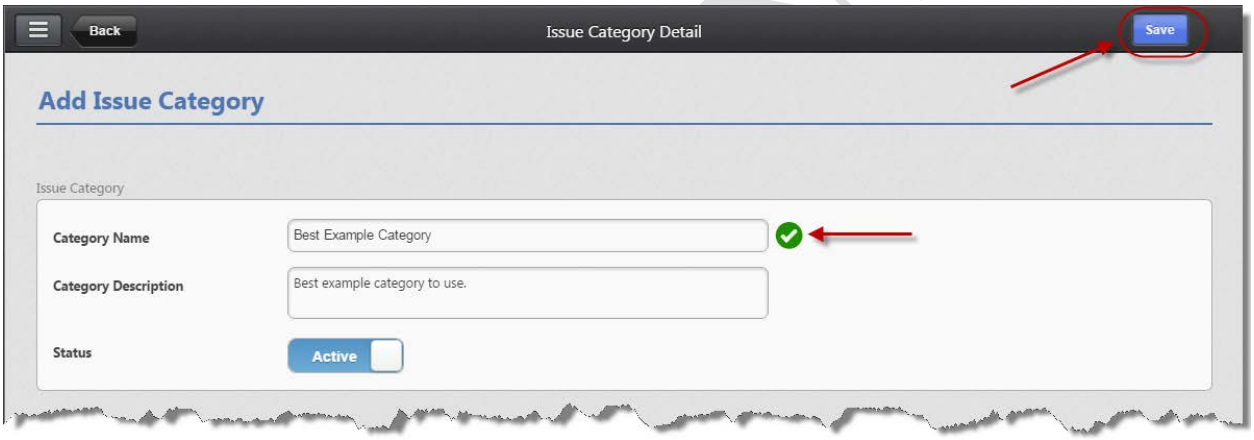
1. Select the **Issue Categories** link. The Issue Category list will display.

   By default, there is one system defined category; however, your institution may elect to create additional categories to be used during the creation of issues.

CONFID

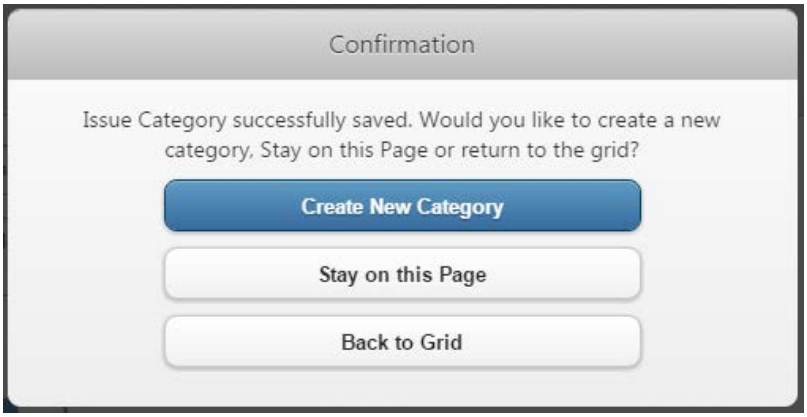


2. To create a new issue category, click on the **plus sign**. The Issue Category Details page will display.
3. The Category Name is required. The description is optional and by default, the Status is set to inactive. Make any necessary changes.



- Category Name
  - The category name is required to create a category. The category name must be unique within the client. This field can contain a maximum of 50 alphanumeric characters.
- Category Description
  - This optional field can contain a maximum of 100 alphanumeric characters.
- Status
  - This field will be a toggle with the option to select a status of active or inactive. The default will be set to active.
  - An inactive category will not be available for assignment to an issue. Inactive categories can be reactivated.

4. The **Save** button will be enabled once a Category Name is chosen. You can return to the category detail page to make changes at any time. When the Save button is clicked a message will be displayed: Issue Category successfully saved. Would you like to create a new item or return to the grid?'


Confirmation
Issue Category successfully saved. Would you like to create a new category, Stay on this Page or return to the grid?
Create New Category
Stay on this Page
Back to Grid

- Clicking *'Create New Category'* will give the user the ability to create a new category.
- Clicking *'Stay on this Page'* will allow the user to remain on the current page with the newly created issue category.
- Clicking *'Back to Grid'* will direct the user back to the Issue Categories page to view the newly created category in the list.

If a user tries to navigate away from the Category Details page without saving, the following message will appear: 'You have unsaved changes. Are you sure you want to leave the page?'

- Clicking *'Ok'* will allow the user to leave the page and discard any changes made.
- Clicking *'Cancel'* will keep the user on the current page.

Important Note: Categories cannot be deleted.

Editing an Issue Category

A custom added category can be edited at any time. With the exception of the category type, all other category fields are editable. To retain changes select the **Save** button prior to leaving the Category Detail Page.

Important Note: No field is editable for the system defined category.

This completes the Controls and Response section.

CONFIDENTIAL

Technical Support and Contact Information

Please feel free to contact our support team with any questions, concerns, or comments you may have regarding this document or the application. All communications from our customers are always welcome and greatly appreciated.

Phone: (888) 494-8449, and press Option 3

Email: customersupport@csiweb.com

Mailing Address:

CSI Regulatory Compliance

13860 Ballantyne Corporate Place

Suite 200

Charlotte, NC 28277

CONFIDENTIAL